Supreme Court, U.S.
FILED

No. 4

031579 MAY 24 2004

OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,
Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,
Respondent.

Petition for a Writ of Certiorari to the United States Court of Appeals for the District of Columbia Circuit

---

PETITION FOR A WRIT OF CERTIORARI

STANLEY PIERRE-LOUIS
LINDA J. ZIRKELBACH
RECORDING INDUSTRY
ASSOCIATION OF AMERICA, INC.
1330 Connecticut Avenue, NW
Suite 300
Washington, D.C. 20036
(202) 775-0101

DONALD B. VERRILLI, JR.
Counsel of Record
THOMAS J. PERRELLI
DEANNE E. MAYNARD
JARED O. FREEDMAN
JENNER & BLOCK LLP
601 Thirteenth Street, NW
Washington, D.C. 20005
(202) 639-6000

Counsel for Petitioner

May 24, 2004

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20001

QUESTION PRESENTED

Whether, contrary to the views of both the United States and the Copyright Office, § 512(h) of the Digital Millennium Copyright Act precludes copyright holders from obtaining the identity of a copyright infringer through issuance of a subpoena to the infringer's Internet service provider, simply because the infringing material is stored on the infringer's computer rather than on the service provider's server.

PARTIES TO THE PROCEEDING

Petitioner Recording Industry Association of America, Inc. was the appellee below. Verizon Internet Services, Inc. was the appellant. The United States intervened to defend the constitutionality of the Digital Millennium Copyright Act.

RULE 29.6 DISCLOSURE

Petitioner is a not-for-profit corporation. It has no parent corporation and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

QUESTION PRESENTED i
PARTIES TO THE PROCEEDING ii
RULE 29.6 DISCLOSURE ii
TABLE OF AUTHORITIES vi
OPINIONS BELOW 1
JURISDICTION 1
STATUTORY PROVISIONS INVOLVED 1
STATEMENT OF THE CASE 2
A. Factual Background 3
1. Copyright Piracy on the Internet 3
2. The DMCA 7
3. The Subpoenas in this Case 10
B. The Proceedings Below 11
1. The District Court's Decisions 11
2. The D.C. Circuit's Decision 12
C. Other DMCA Subpoena Proceedings 14
REASONS FOR GRANTING THE PETITION 15
A. Internet Piracy Of Copyrighted Works Is A Huge And Growing Social Problem. 17
B. The Decision Below Is Inconsistent With The Text, Structure, And Purposes Of Section 512(h). ... 19

C. The DMCA Expressly Addressed Piracy Over Conduit Facilities And The D.C. Circuit Effectively Repealed Congress' Solution. 25

D. Review Is Urgently Needed.....27

CONCLUSION 29

APPENDIX A

Recording Industry Ass'n of America v. Verizon Internet Services, Inc., Opinion (D.C. Cir. Dec. 19, 2003) 1a

APPENDIX B

In re Verizon Internet Services, Inc., Opinion (D.D.C. Jan. 21, 2003) 18a

APPENDIX C

In re Verizon Internet Services, Inc., Opinion (D.D.C. Apr. 24, 2003).....55a

APPENDIX D

Denial of Petition for Rehearing, *Recording Industry Ass'n of America v. Verizon Internet Services, Inc.* (D.C. Cir. Feb. 24, 2004).....112a

APPENDIX E

Denial of Petition for Rehearing En Banc, *Recording Industry Ass'n of America v. Verizon Internet Services, Inc.* (D.C. Cir. Feb. 24, 2004).....113a

APPENDIX F

17 U.S.C. § 512 ..... 114a

APPENDIX G

Letter from Scott R. McIntosh, Department of Justice, to Mark Langer, Clerk of the United States Court of Appeals for the D.C. Circuit, of Sept. 22, 2003 ..... 133a

APPENDIX H

Statement by Marybeth Peters, The Register of Copyrights, *Before the Senate Comm. on the Judiciary*, 108th Cong. (Sept. 9, 2003) 135a

TABLE OF AUTHORITIES

CASES

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) 7, 17

Allied-Bruce Terminix Cos. v. Dobson, 513 U.S. 265 (1995) 23

Batjac Productions Inc. v. GoodTimes Home Video Corp., 160 F.3d 1223 (9th Cir. 1998) 16

Bonneville International Corp. v. Peters, 153 F. Supp. 2d 763 (E.D. Pa. 2001), *aff'd*, 347 F.3d 485 (3d Cir. 2003) 16

Carson Harbor Village, Ltd. v. Unocal Corp., 270 F.3d 863 (9th Cir. 2001) 23

FBI v. Abramson, 456 U.S. 615 (1982) 24

General Dynamics Land Systems, Inc. v. Cline, 124 S. Ct. 1236 (2004) 23

Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985) 18

Holloway v. United States, 526 U.S. 1 (1999) 23

Natural Resources Defense Council, Inc. v. U.S. EPA, 907 F.2d 1146 (D.C. Cir. 1990) 23

Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) 5

Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) 5

Satellite Broadcasting & Communications Ass'n of America v. Oman, 17 F.3d 344 (11th Cir. 1994) 16

Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994) 5

United States v. Bisceglia, 420 U.S. 141 (1975) 24

United States v. Hill, 79 F.3d 1477 (6th Cir. 1996) 23

United States v. Morton, 467 U.S. 822 (1984) 23

United States v. Stowe, No. 96 C 2702, 1996 WL 467238 (N.D. Ill. Aug. 15, 1996) 5

STATUTES

17 U.S.C. § 512 ..... *passim*

17 U.S.C. § 512(a) 8, 13, 20, 25

17 U.S.C. § 512(b) 8, 13, 21

17 U.S.C. § 512(c) 8, 13, 21

17 U.S.C. § 512(c)(3)(A) 12, 20, 21, 22, 23

17 U.S.C. § 512(c)(3)(A)(iii) 12, 21

17 U.S.C. § 512(d) 8, 13, 21

17 U.S.C. § 512(h) ..... *passim*

17 U.S.C. § 512(h)(1) 9

17 U.S.C. § 512(h)(4) 9

17 U.S.C. § 512(h)(5) 9, 21, 22

17 U.S.C. § 512(i)(1)(A) 8

17 U.S.C. § 512(j) 13, 22, 23

17 U.S.C. § 512(k)(1)(A) 20

17 U.S.C. § 512(k)(1)(B) 20

LEGISLATIVE MATERIAL

H.R. Rep. No. 105-551(II) (1998) 20

S. Rep. No. 105-190 (1998) 2, 6, 8

Copyright Piracy, and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (Sept. 11, 1997) 3, 6

NII Copyright Protection Act of 1995 (Part 2): Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 104th Cong. (Feb. 7-8, 1996) 6, 26

Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (Sept. 16-17, 1997) 6, 7

The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Senate Comm. on the Judiciary, 105th Cong. (Sept. 4, 1997) 6, 7, 9

Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Comm. on Governmental Affairs, 108th Cong. (Sept. 30, 2003), *available at* http://govt-aff.senate.gov/index.cfm?Fuseaction=Hearings.Testimony&HearingID=120&WitnessID=414 ..... 17, 18

Statement by Marybeth Peters, The Register of Copyrights, *Before the Senate Comm. on the Judiciary*, 108th Cong. (Sept. 9, 2003), *available at* http://www.copyright.gov/docs/regstat090903.html 2

MISCELLANEOUS

Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring over the Internet*, 18 Hastings Comm. & Ent. L.J. 729 (Summer 1996) 4

Edison Media Research Study (June 2003) 18

Benny Evangelista, *Download That Tune*, S.F. Chron., Dec. 3, 1998 7

Lev Grossman, *It's All Free*, Time, May 5, 2003 17

Andrew Leonard, *Mutiny on the Net*, Salon, March 1998, *available at* http://archive.salon.com/21st/feature/1998/03/cov_20feature.html 4

The Music Industry, The Economist, Oct. 31, 1998 3

Andy Patrizio, *Cyberchatters Trade Electronic Booty*, CMP TechWeb, Dec. 30, 1998 5

Pew Internet & American Life Project, *The Impact of Recording Industry Suits Against Music File Swappers* (Jan. 2004), *available at* http://www.pewinternet.org/reports/pdfs/PIP_File_Swapping_Memo_0104.pdf 27

T.R. Reid, *Power Computing*, Wash. Post, Dec. 2, 1991 4

Chris Sherman, *Napster: Copyright Killer or Distribution Hero?*, Online, Nov. 1, 2000 7

Kenneth D. Suzan, *Tapping to the Beat of a Digital Drummer: Fine Tuning U.S. Copyright Law for Music Distribution on the Internet*, 59 Alb. L. Rev. 789 (1995) 4

Third Largest BBS in US Hit in FBI Raid, Newsbyte, Feb. 19, 1993 5

www.riaa.com/news/newsletter/pdf/2003yearEnd.pdf 18

PETITION FOR A WRIT OF CERTIORARI

The Recording Industry Association of America, Inc. ("RIAA") respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the District of Columbia Circuit in this case.

OPINIONS BELOW

The opinion of the D.C. Circuit is reported at 351 F.3d 1229 (D.C. Cir. 2003), and is reprinted at Pet. App. 1a-17a. That court's order denying RIAA's petition for rehearing is reprinted at Pet. App. 112a, and its order denying RIAA's petition for rehearing en banc is reprinted at Pet. App. 113a. The opinions of the United States District Court for the District of Columbia are reported at 240 F. Supp. 2d 24 (D.D.C. 2003) and 257 F. Supp. 2d 244 (D.D.C. 2003), and are reprinted at Pet. App. 18a-54a and 55a-111a.

JURISDICTION

The D.C. Circuit issued its decision on December 19, 2003. It denied RIAA's timely petition for rehearing or rehearing en banc on February 24, 2004. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1254(1).

STATUTORY PROVISIONS INVOLVED

This case involves Title II of the Digital Millennium Copyright Act, 17 U.S.C. § 512, reprinted at Pet. App. 114a-132a.

STATEMENT OF THE CASE

This case involves a question of exceptional importance under the Digital Millennium Copyright Act ("DMCA"). Congress enacted the DMCA to combat the emerging reality of "massive piracy" of copyrighted works on the Internet. S. Rep. No. 105-190, at 8 (1998) ("S. Rep."). In Title II of the DMCA, codified at 17 U.S.C. § 512, Congress conferred upon Internet service providers ("ISPs") certain limitations on liability in exchange for requiring ISPs to cooperate with copyright owners to combat copyright piracy by users of their networks. *See* S. Rep. at 40-41. The core of the congressional bargain struck in § 512 is that copyright owners must generally seek redress in the first instance against infringing users, not ISPs, and that ISPs must assist copyright owners' efforts to do so.

As the Copyright Office has explained, "[a]mong those balancing obligations" Congress imposed on ISPs in exchange for limiting their copyright liability "was the requirement that ISPs 'expeditiously' respond to subpoenas to provide identifying information about subscribers accused of copyright infringement so that the controversy could be settled in court." *See* Statement by Marybeth Peters, The Register of Copyrights, *Before the Senate Comm. on the Judiciary*, 108th Cong. (Sept. 9, 2003), *available at* http://www.copyright.gov/docs/regstat090903.html, at Pet. App. 142a. That obligation is set forth in § 512(h) of the DMCA.

The decision below eviscerates the subpoena authority conferred by Congress in § 512(h), and thereby undoes the fundamental bargain at the heart of the DMCA. The D.C. Circuit held that a § 512(h) subpoena cannot issue unless the infringing material is stored on the ISP's own server, even though the text of § 512(h) contains no such limitation, and even though the vast majority of infringing material on the

Internet is stored on home computers or other computers not controlled by ISPs. Moreover, the D.C. Circuit's decision conflicts with the position of the United States and the Copyright Office. As the United States has explained, "the D.C. Circuit has impaired the Copyright Act's basic mechanisms for protecting intellectual property rights," and "fatally compromise[d]" private copyright enforcement against Internet infringers. Br. for the United States as Intervenor and *Amicus Curiae, RIAA v. Charter Communications, Inc.*, No. 03-3802, at 13, 16 (8th Cir. filed Feb. 24, 2004) ("US Charter Br."), *available at* http://www.ca8.uscourts.gov/briefs/04/03/intervenor/033802_1br.pdf?A1=View+Brief. Immediate review is needed because the decision below is thwarting legitimate efforts across the nation to combat ongoing piracy that is causing irreparable harm to copyright owners on an unprecedented scale.

A. Factual Background

1. Copyright Piracy on the Internet

Congress enacted the DMCA in 1998. By that time, copyright piracy on the Internet had already reached epidemic proportions – approximately 3 million sound recordings were being downloaded from the Internet every day, the vast majority of which were pirated. *See The Music Industry*, The Economist, Oct. 31, 1998, at 67. Armed with a personal computer and a connection to the Internet, an individual could unlawfully disseminate copyrighted works (such as music, movies or software) to millions of people with just a few keystrokes. As the Copyright Office explained in 1997, "a disgruntled former employee, a dissatisfied customer, [or] an Internet user opposed to the fundamental concepts of copyright law" could inflict "tremendous damage to the market for a copyrighted work." *Copyright Piracy, and H.R. 2265, The No Electronic*

Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. 9 (Sept. 11, 1997) (Marybeth Peters, Register of Copyrights).

Well before enactment of the DMCA, much of the infringement occurring on the Internet involved individuals storing infringing material on their personal computers, and using ISP networks merely as a conduit to disseminate that material. As early as the 1980s, Internet users were "posting" copyrighted works on electronic bulletin boards ("BBSs").[1] By the thousands, users transformed their own computers into BBSs or file transfer protocol ("FTP") sites from which others could download copyrighted material.[2] By the mid-1990s, it was commonplace for Internet users to exchange copyrighted works by e-mail[3] or Internet Relay

---

[1] A BBS allows users to post files for others to download. A BBS requires inexpensive software, a home computer, and a telephone line. *See* T.R. Reid, *Power Computing*, Wash. Post, Dec. 2, 1991, at F18 ("If you have a telephone, a personal computer and about $100 to cover start-up costs, you can broadcast to a national audience as early as tomorrow by going on-line with your own BBS.").

[2] FTP software turns any computer into a server that allows others to download files, including perfect digital copies of copyrighted sound recordings. *See* Andrew Leonard, *Mutiny on the Net*, Salon, March 1998, *at* http://archive. salon.com/ 21st/ feature /1998/03/cov_20feature.html (FTP software "allows anyone with a computer and a modem to make [pirated music] files on their home computer accessible to the [Internet]").

[3] *See* Kenneth D. Suzan, *Tapping to the Beat of a Digital Drummer: Fine Tuning U.S. Copyright Law for Music Distribution on the Internet*, 59 Alb. L. Rev. 789, 807 (1995) ("It is quite feasible for someone to download a song from a commercial site such as CompuServe and then e-mail or post the 'digitized audio file' on a bulletin board for others to copy. In essence, 'there is no way to ensure that a teen-ager who buys a new record will not send it to 1,000 of her closest friends.'") (internal citation omitted); Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct*

Chat ("IRC").[4] Although these technologies involved the use of ISPs to transmit data, ISPs generally did not store the infringing material on their servers. And for infringers, these technologies offered the added advantage of anonymity.

In the early 1990s, copyright owners began suing to stop Internet infringement, targeting BBSs operated from personal computers connected to the Internet by ISPs. *E.g., Sega Enters. Ltd. v. MAPHIA*, 857 F. Supp. 679, 682-83 (N.D. Cal. 1994); *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1555-56 (M.D. Fla. 1993). In some cases, copyright owners sued both the person running the BBS and the ISP that linked the BBS to the Internet. *E.g., Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). As early as 1993, the Department of Justice prosecuted infringers who offered pirated software from BBSs operated from home computers. *E.g., United States v. Stowe*, No. 96C2702, 1996 WL 467238, at *1 (N.D. Ill. Aug. 15, 1996).[5]

By 1998 when the DMCA was enacted, Congress had amassed an enormous legislative record relating to Internet piracy. That record documents infringement by ISP subscribers using their personal computers to disseminate

---

Occurring over the Internet, 18 Hastings Comm. & Ent. L.J. 729, 737 (Summer 1996) ("[I]n a matter of seconds and at a cost of mere pennies," a copyrighted work can be transmitted "via E-mail to thousands of people.").

[4] IRC allows users to communicate and exchange copyrighted files directly with each other, without posting information on a server. *See* Andy Patrizio, *Cyberchatters Trade Electronic Booty*, CMP TechWeb, Dec. 30, 1998.

[5] *See also Third Largest BBS in US Hit in FBI Raid*, Newsbyte, Feb. 19, 1993 (describing raid of home BBS utilizing 125 computers and causing millions of dollars in copyright theft).

copyrighted material directly to others, using the ISP's network merely as a conduit. The Department of Justice testified about infringement committed from FTP and BBS sites run on personal computers. *See Copyright Piracy, and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 17-18 (Sept. 11, 1997) (Kevin DiGregory, Deputy Assistant Attorney General, Department of Justice) ("DiGregory Testimony"). ISP witnesses testified about the *Sega, Playboy* and *Netcom* cases – all of which involved infringing activity on personal computers linked by ISPs to the Internet – because these cases suggested that ISPs could be held liable for merely transmitting information from one infringing user to another.[6] Congress also heard testimony about the "growing use of 'blanket' e-mail messages" to commit copyright infringement and about infringers using e-mail (and attachments) to disseminate hundreds of copyrighted software programs.[7] One songwriter explained that e-mail distribution systems were difficult to police because ISPs

---

[6] *See, e.g.*, S. Rep. at 19 n.20 (noting *Netcom* and *Playboy*); *The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 101-03 (Sept. 4, 1997) (George Vradenburg, General Counsel, America Online, Inc.) (discussing *Netcom* and *Sega*).

[7] *Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 175 (Sept. 16-17, 1997) (Ronald Dunn, President, the Information Industry Association); *NII Copyright Protection Act of 1995 (Part 2): Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 88 (Feb. 7-8, 1996) (Garry L. McDaniels on behalf of the Software Publishers Association); *see* DiGregory Testimony, at 17-18 (describing use of e-mail to commit infringement of software programs).

had no obligation to reveal the identities of e-mail customers, absent a court order.[8]

As technology has advanced, digital piracy has continued to grow. In 1998, a new compressed digital format – mp3 – became the medium of choice for infringers. *See* Benny Evangelista, *Download That Tune*, S.F. Chron., Dec. 3, 1998, at A1. Very soon thereafter, peer-to-peer ("P2P") systems emerged. P2P systems – like their technological predecessors BBS, FTP and IRC software – allow users, under the cloak of anonymity, to disseminate files stored on their personal computers (and not on their ISP's server) to other Internet users.[9]

2. The DMCA

In Title II of the DMCA, 17 U.S.C. § 512, Congress sought to address the two principal (and interrelated) issues raised by copyright infringement on the Internet: ISPs' fear of liability for infringement committed by users of their networks,[10] and copyright owners' need for tools to combat

---

[8] *See Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 160 (Sept. 16-17, 1997) (Allee Willis).

[9] Napster was the first and most notorious P2P system, until the courts shut it down. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). The Napster P2P system simply merged FTP software (which can turn a personal computer into a server that allows Internet users to download files) and IRC software (which enables direct communication among Internet users). *See* Chris Sherman, *Napster: Copyright Killer or Distribution Hero?*, Online, Nov. 1, 2000. As discussed above, both of these technologies were used for copyright piracy on the Internet well before the enactment of the DMCA. Other P2P systems have arisen in Napster's wake including Kazaa, Grokster and Gnutella.

[10] *See, e.g., The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 32 (Sept. 4, 1997) (Roy Neel, President, United States Telephone Association) (claiming that copyright owners should sue direct infringers transmitting

this "massive piracy." S. Rep. at 8.[11] Section 512 creates a balanced system of "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." *Id.* at 40. ISPs received new protections that limit their liability for their subscribers' infringement. In exchange, Congress imposed obligations on ISPs to assist copyright owners in combating such infringement.

The protections given to ISPs are set forth in subsections (a)-(d) of § 512, which establish four distinct limitations on liability for infringement. Each limitation applies to a particular ISP function. Subsection (a) limits the liability of ISPs that transmit infringing material – that is, when the ISP is a mere conduit. Subsections (b), (c), and (d) limit the liability of ISPs when they are caching, storing, or linking to infringing material. §§ 512(b) (caching), 512(c) (storing), 512(d) (linking).

Congress made these protections conditional. ISPs can claim them only if they take statutorily prescribed steps to assist copyright owners in policing against infringement. To qualify for any of the limitations on liability, an ISP must maintain and enforce a policy of terminating the accounts of subscribers who are "repeat infringers." § 512(i)(1)(A). To retain the limitations in subsections (b)-(d) (which cover storage functions), an ISP must also promptly remove or disable access to infringing material stored on its servers upon receiving a notification of infringement. The DMCA does not require an ISP to take any of these steps; rather,

---

copyrighted materials, not the ISPs themselves); *id.* at 102 (Vradenburg) (claiming that such liability would "wreak havoc" on ISPs).

[11] *See The Copyright Infringement Liability of Online and Internet Service Providers: Hearing Before the Senate Comm. on the Judiciary*, 105th Cong. 15 (Sept. 4, 1997) (Cary Sherman, General Counsel, RIAA).

failure to do so results in the loss of the limitations on liability.

In addition, Congress imposed on ISPs the obligation that is at issue in this case – namely, the duty to disclose to copyright owners the identity of subscribers using their networks to infringe. That duty is not conditional. Under § 512(h), a copyright owner or its agent may request that "the clerk of any United States district court" issue a subpoena requiring an ISP to disclose the identity of such infringers when the copyright owner documents good faith claims of infringement. § 512(h)(1). The clerk is under a mandatory duty to issue the subpoena "expeditiously," and the ISP is likewise under a mandatory duty to respond to it "expeditiously." § 512(h)(4); § 512(h)(5).

Section 512(h) is essential to combat the Internet copyright piracy that Congress aimed to prevent. As the Copyright Office has explained, "[i]t is common sense that in order to be able to take action against the users of peer-to-peer networks, the copyright owner must know who those users are." Pet. App. 141a (internal endnote omitted). Only ISPs know the identities of subscribers using their networks to infringe. Copyright owners therefore need to obtain that information from the ISP. "Congress foresaw this need and addressed it by including in the DMCA a process by which copyright owners can learn basic identifying information about alleged infringers from their internet service providers . . . ." *Id.* (internal endnote omitted).

On its face, this subpoena provision applies to all ISPs. As the Copyright Office has explained, ISPs who are conduits of infringing material "received the benefits and burdens of the same bargain that service providers engaged in the other activity covered by 512 received. In exchange for a powerful limitation on liability, they undertook some obligations, including the obligation to identify alleged

infringers when served with a subsection 512(h) subpoena." Pet. App. 143a.

3. The Subpoenas in this Case

In the four years after enactment of the DMCA, RIAA served approximately 100 DMCA subpoenas, 60 of which involved infringing material that was not stored on an ISP's server. Second Declaration of Frank Creighton at 6-7 (Joint Appendix at JA424-JA425 (D.C. Cir. filed July 9, 2003)). At no point did any ISP object on the ground that § 512(h) did not apply to ISPs that are not storing infringing material on their own servers. *Id.*

In July 2002, RIAA discovered an individual illegally disseminating over 600 copyrighted sound recordings without authorization. RIAA discovered this infringer by logging onto a P2P network and observing the individual offering the copyrighted works. RIAA recorded the Internet Protocol ("IP") address and screen name of the copyright infringer, the date and time at which the infringer engaged in unlawful conduct, and the particular sound recordings the infringer was unlawfully disseminating.[12] From the IP address, RIAA could determine that the infringer was using Verizon's network to disseminate the copyrighted works. On July 24, 2002, RIAA sought and obtained a subpoena pursuant to § 512(h) requiring Verizon to disclose the identity of the infringer. On February 4, 2003, RIAA obtained a second subpoena seeking the identity of another Verizon subscriber who was disseminating more than 800 copyrighted works. Pet. App. 4a-5a, 23a, 58a.

---

[12] An IP address is a number that specifically identifies a particular computer using the Internet.

B. The Proceedings Below

1. The District Court's Decisions

Verizon objected to the first subpoena on the ground that § 512(h) authorizes subpoenas only to ISPs storing infringing material on their own networks. The district court rejected "Verizon's strained reading of the Act," Pet. App. 31a, explaining that "nothing in the language or structure of the statute . . . suggests Congress intended the DMCA" to be restricted in that manner. *Id.* at 37a. The court held that the text of § 512(h) made clear that it applied to *all* ISPs, and emphasized that the definition of the term "service provider" used in § 512(h) encompassed all ISPs, including pure conduits. *Id.* at 27a-30a.

In rejecting Verizon's interpretation, the district court concluded that there is "no sound reason why Congress would enable a copyright owner to obtain identifying information from a service provider storing infringing material on its system, but would not enable a copyright owner to obtain identifying information from a service provider transmitting the material over its system." *Id.* at 36a. Indeed, Verizon's position "would create a huge loophole in Congress's effort to prevent copyright infringement on the Internet," because "the largest opportunity for copyright theft is through [P2P] software." *Id.*

Thereafter, Verizon moved to quash the second subpoena on the grounds that the subpoenas violated Article III and the First Amendment to the Constitution. The district court rejected those arguments as well. *Id.* at 59a-96a.

2. The D.C. Circuit's Decision

The D.C. Circuit reversed. The Circuit held that § 512(h) does not authorize subpoenas to an ISP that serves as a conduit for infringing material, but does not store the material on its servers. *Id.* at 6a.

In reaching that result, the D.C. Circuit gave no weight to the fact that the term "service provider," as used in § 512(h), is expressly defined to include all ISPs performing all functions, including conduit functions. The court concluded that the defined term should not be given its full scope, but was instead subject to a categorical limitation. That limitation, the court believed, arose from the cross-reference in § 512(h) to another DMCA provision, § 512(c)(3)(A). Section 512(c)(3)(A) requires copyright owners seeking a subpoena to serve upon ISPs a notification that documents the good faith basis for their claim of infringement by, *inter alia*, describing "the infringing material to be removed or access to which is to be disabled." 17 U.S.C. § 512(c)(3)(A)(iii). The court read that provision not as a notification requirement, but instead as a categorical limitation on the substantive scope of the statutory subpoena power. The court was of the view that "Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers." Pet. App. 9a-10a. The court then drew from that observation the conclusion that a copyright holder could never "satisf[y]" the requirements of subsection (c)(3)(A)(iii) sufficient to obtain a subpoena when infringing material is stored on a subscriber's computer rather than an ISP's server. *Id.* at 12a. Thus, the court concluded, Congress intended to impose on ISPs a duty to respond to § 512(h) subpoenas only when the ISP actually stored infringing material on its network.

Although the appeals court acknowledged the district court's common-sense holding that an ISP can "disable access" to infringing material on a subscriber's home computer by terminating the subscriber's Internet access (*see* Pet. App. 33a & n.5), it nevertheless held that termination of an account did not constitute "disabl[ing] access" in satisfaction of § 512(c). *Id.* at 10a. To support that counterintuitive view, the court looked to yet another provision of § 512: subsection (j). That subsection prescribes the types of injunctive relief that can be entered against ISPs that qualify for the safe harbors of § 512(a)-(d). Because Congress purportedly used the terms "disabl[ing] access" and "terminating" accounts to mean different things in subsection (j), the D.C. Circuit presumed that the statutory terms must have mutually exclusive meanings – without considering whether the two terms could have overlapping meanings. *Id.*

Moreover, in addition to its purported reliance on the plain language of the statute, the D.C. Circuit invoked "the legislative history of the DMCA" which, the court asserted, "betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works." *Id.* at 14a. Apparently unaware of the legislative history documenting Congress' concern with Internet piracy involving material stored on home computers, the court believed that Congress did not "draft the DMCA broadly enough to reach [P2P] technology when it came along." *Id.* at 15a. The court acknowledged that the effect of this ruling was to deprive copyright owners of the primary tool § 512 gave them to combat Internet piracy, but believed that the purported gap in the statute's protective scheme could only be filled by Congress. *Id.* at 16a.

RIAA filed a timely petition for rehearing or rehearing en banc, which the D.C. Circuit denied on February 24, 2004. Pet. App. 112a-113a.

C. Other DMCA Subpoena Proceedings

In addition to the subpoenas at issue in this case, subpoena enforcement proceedings raising identical issues are pending in at least two other courts. *See RIAA v. Charter Communications, Inc.*, No. 03-3802 (8th Cir.); *In re Subpoena to Univ. of North Carolina*, No. 1:03MC138 (M.D.N.C.); *In re Subpoena to North Carolina State Univ.*, No. 1:03MC139 (M.D.N.C.). After the D.C. Circuit issued its decision, the United States joined the proceedings in the Eighth Circuit and in the North Carolina district court to support enforcement of the subpoenas. In those proceedings, the United States has taken the position that the D.C. Circuit's interpretation of § 512(h) is in error, and that the provision authorizes subpoenas to obtain the identities of ISP subscribers who store infringing material on their personal computers rather than on their ISPs' servers. *See* US Charter Br. at 16-33. The Copyright Office of the United States also interprets § 512(h) as requiring ISPs to disclose the identity of subscribers who store infringing material on their personal computers, in direct conflict with the D.C. Circuit's reading of § 512(h). Pet. App. 141a-144a.[13]

---

[13] The United States briefed only the constitutional issues before the D.C. Circuit and did not address the statutory question. In response to a question at oral argument, counsel for the United States informed the D.C. Circuit that the Copyright Office interprets the statute as RIAA does, and subsequently confirmed that position by letter. Pet. App. 133a-134a. After the D.C. Circuit ruled, the Department of Justice filed *amicus* briefs in the proceedings discussed above. Those briefs set forth the position of the United States with respect to the meaning of § 512(h), which is in accord with that of the Copyright Office.

REASONS FOR GRANTING THE PETITION

The decision below gutted a federal statute essential to protecting intellectual property rights from piracy on the Internet. Section 512(h) imposes on all "service providers" the duty to respond to subpoenas seeking the identity of subscribers who use the ISP's network to commit copyright infringement. Yet the D.C. Circuit read § 512(h) as not reaching infringement by ISP subscribers who store the infringing material on their own systems – by far the largest category of Internet infringement. Despite conceding that its interpretation left copyright holders without "the legal tools" needed to combat "widespread infringement," Pet. App. 16a, the D.C. Circuit purported to find in the statutory text a clear instruction from Congress to limit § 512(h) in a manner that defeats the very purpose for which it was enacted. By failing to give effect to the plain language of § 512(h) itself, and instead divining from a statutory cross-reference an implied limitation on the expressly defined scope of that provision, the D.C. Circuit has eliminated the primary tool Congress provided to facilitate vigorous private copyright enforcement against Internet infringers.

There is a pressing need for immediate review of the D.C. Circuit's decision. As that court itself recognized, "[t]he stakes are large for the music, motion picture, and software industries and their role in fostering technological innovation." Pet. App. 16a. The district court similarly observed that "copyright infringement and piracy of music recordings over the Internet has skyrocketed, resulting in enormous losses for the industry," and the value of copyrighted works "could plummet" if "universal downloading could continue unabated." *Id.* at 106a. The D.C. Circuit's decision is having the effect of depriving copyright owners of the ability to expeditiously obtain subpoenas not only in the District of Columbia but

throughout the nation. That is crippling the private copyright enforcement that Congress envisioned as a bulwark against Internet lawlessness, and allowing Internet piracy to metastasize.

Moreover, the harms are not confined to copyright owners. The epidemic of Internet piracy threatens important public interests as well. Our copyright system is, as this Court has repeatedly recognized, an "engine of free expression" and that system is under assault by the conduct that Congress enacted § 512(h) to help combat. Even more fundamentally, allowing massive, anonymous Internet piracy to continue unchecked has a corrosive effect on bedrock commitments to the rule of law and protection of private property on the Internet.

Indeed, in recognition of the public importance of the issue this case presents, the United States has taken the unusual step of participating in multiple proceedings involving private litigants to explain that "the D.C. Circuit's statutory ruling in [this case] is inconsistent with the text of Section 512(h) and the legislative policies that underlie it." US Charter Br. at 12. As the United States has explained in these cases, the D.C. Circuit's decision conflicts with the interpretation of the Copyright Office, which reads "the plain language of subsection 512(h)" as applying to "'all service providers, regardless of the functions a service provider may perform . . . .'" Pet. App. 142a-143a (quoting Pet. App. 28a).[14]

---

[14] That view is entitled to deference. *Batjac Prods. Inc. v. GoodTimes Home Video Corp.*, 160 F.3d 1223, 1230 (9th Cir. 1998); *Satellite Broad. & Communications Ass'n of Am. v. Oman*, 17 F.3d 344, 347-48 (11th Cir. 1994). Deference is particularly warranted in this case because the Copyright Office "played a formative role" in drafting and implementing the

No offsetting consideration favors delaying review. The issue this case raises will recur; indeed it is already recurring. Further adjudication is not likely to shed additional light on the question presented, which involves a straightforward issue of statutory construction. Nor are the factual circumstances of this case anomalous or unusual. To the contrary, the facts here are typical of any case that will present these important issues.

A. Internet Piracy Of Copyrighted Works Is A Huge And Growing Social Problem.

Copyright piracy on peer-to-peer networks is the greatest current threat to the integrity of copyright in the digital age. Use of peer-to-peer networks is growing by leaps and bounds: there are now more than five million people on peer-to-peer networks at any given moment. *See Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Comm. on Governmental Affairs*, 108th Cong. (Sept. 30, 2003) (statement by Mitch Bainwol, CEO, RIAA), *available at* http://govt-aff.senate.gov/index.cfm?Fuseaction=Hearings.Testimony&HearingID=120&WitnessID=414 ("Bainwol Statement"). Approximately 90% of the content on P2P systems is copyrighted movies, software, images, and music disseminated without authorization. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001). More than *2.6 billion* infringing music files are downloaded each month. Lev Grossman, *It's All Free*, Time, May 5, 2003. Internet piracy has become big business, as companies have sprung up to cater to the illicit trade in copyrighted

---

DMCA. *Bonneville Int'l Corp. v. Peters*, 153 F. Supp. 2d 763, 772 (E.D. Pa. 2001), *aff'd*, 347 F.3d 485 (3d Cir. 2003).

material.[15] ISPs also profit handsomely. P2P users drive the demand for broadband services, such as Verizon's DSL, which offer faster speeds for Internet access and downloading.

This piracy is inflicting massive and irreparable harm. The link between P2P piracy and lost sales is well documented. Among the heaviest downloaders, purchases of compact discs declined by 61% from 2002 to 2003. *See* Edison Media Research Study (June 2003). Not surprisingly, retail sales of music have plummeted, falling 7% in 2000, 10% in 2001, 11% in 2002, and 7% in 2003. *See* http://www.riaa.com/news/newsletter/pdf/2003yearEnd.pdf. Of particular note is the precipitous drop in sales of the CDs that are most popular and most commonly disseminated on peer-to-peer networks: from 2000 to 2002, sales of the top 10 selling albums dropped almost 50%. *See* Bainwol Statement, *supra*.

The issue presented here thus arises in a context of great national significance. Massive copyright infringement on the Internet not only directly harms all of the American industries that rely on intellectual property for their livelihood, but also poses a direct threat to the freedom of expression, *see Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 558 (1985), and indeed to the very notion of respect for private property and for the rule of law on the Internet.

Copyright owners cannot fight back unless they know who the infringers are. Congress understood this. That is

---

[15] Peer-to-peer companies themselves (often headquartered abroad in small island nations) receive millions of dollars annually for advertising to P2P users and for installing spyware on users' computers, which gathers personal information for marketing and other purposes. *See, e.g.*, www.kazaa.com; www.grokster.com.

why § 512(h) is in the DMCA. The provision creates a streamlined mechanism for obtaining the identities of infringers, thus allowing copyright owners to move swiftly against those unlawfully disseminating copyrighted works. As both Congress and the district court recognized, expedition is critical because the information that copyright owners need – the identity of the Internet user infringing works from a particular IP address at a given date and time – is maintained by ISPs for only a short period of time; once it is destroyed, the copyright owner can never enforce its rights. Pet. App. 69a.

The D.C. Circuit's opinion blows a hole in § 512(h), rendering it useless where it is most needed and leaving the largest category of Internet infringement beyond the reach of the statute. As the United States has explained, the D.C. Circuit's opinion strikes at the heart of the congressional bargain and "fundamentally alter[s]" the *quid pro quo* embodied in the DMCA. US Charter Br. at 17. With respect to the most common form of infringement, if the D.C. Circuit's interpretation is correct, "the *quid pro quo* exacted by Congress in return for immunity thus turns out to be . . . nothing." *Id.* at 18 (ellipsis in original).

B. The Decision Below Is Inconsistent With The Text, Structure, And Purposes Of Section 512(h).

The D.C. Circuit believed that its perverse result was compelled by the text of § 512(h) and related provisions. But that is not so. As the United States has explained, "[p]roperly read, Section 512(h) applies to ISPs engaged in data transmission as well as to ISPs engaged in data storage and other activities. And only that reading vindicates the policies underlying Title II of the DMCA and the underlying policies of federal copyright law." US Charter Br. at 18-19.

The statute broadly defines the term ISP to include *all* "provider[s] of online services or network access." 17 U.S.C. § 512(k)(1)(B). Nowhere in § 512(h) did Congress draw any distinction between ISPs who store infringing material and those who do not – even though "it would have been a trivial matter to say so." US Charter Br. at 19. As the district court in this case observed, Congress could have stated "such a limitation in subsection (h), or stated that subsection (h) does not apply to subsections (a), (b), or (d), or even have placed the subpoena authority itself within subsection (c). But Congress did not do so." Pet. App. 32a.

In fact, Congress did the opposite. Section 512 contains two separate definitions of "service provider." One of those definitions is the precise limitation adopted by the D.C. Circuit – that is, it narrowly defines service provider to include only ISPs performing the "conduit" function of transmitting information. *See* 17 U.S.C. § 512(k)(1)(A). Congress expressly applied that definition *only to § 512(a). Id.* For all other provisions of § 512 – including § 512(h) – Congress defined service provider to include the broadest possible array of ISPs, including those who are conduits. *See* § 512(k)(1)(B); *see also* H.R. Rep. No. 105-551(II), at 64 (1998) (§ 512(k)(1)(B) definition "includes, for example, services such as providing Internet access, e-mail, chat room and web page hosting services"). Thus, "when Congress identified the entities that are subject to subpoenas under Section 512(h), it used unqualified language that encompasses all ISPs and embraces, rather than excludes, ISPs engaged in data transmission." US Charter Br. at 20 (citation omitted).

Despite the fact that Congress took great care in § 512 generally, and in § 512(h) in particular, to define the scope of an ISP's duties, the D.C. Circuit brushed this statutory definition aside. Calling reliance on the definition "silly," Pet. App. 11a, the D.C. Circuit instead divined a drastic

implied limitation in the scope of the statutory subpoena power based on subsection (h)'s cross-reference to § 512(c)(3)(A). The latter provision prescribes the contents of a notification a copyright owner must provide under § 512 to establish its bona fides as a prelude to enforcing its rights. It is cross-referenced by numerous other subsections of § 512. Its obvious purpose in the § 512(h) context is to establish a basis for the copyright owner's claim that an ISP subscriber has infringed the owner's rights, and thereby to justify the effort to obtain the subscriber's identity.

The D.C. Circuit nevertheless read the provision as an effort on the part of Congress to restrict the subpoena power to situations where the ISP actually stores infringing material. The court did so because one of the required items in a subsection (c)(3)(A) notification is identification of material "that is to be removed or access to which is to be disabled." § 512(c)(3)(A)(iii). That requirement is in the provision because the notification also serves the different function of triggering the ISP's duty to remove or disable material in order to preserve its limitations on liability in subsections (b), (c) and (d) – *see supra* pp. 8-9 – in situations where a copyright owner has invoked those provisions. Ignoring this obvious explanation for the requirements of § 512(c)(3)(A), the court of appeals instead read the provision as an implicit restriction on the substantive scope of the subpoena power. In essence, the court concluded that copyright owners had the right to enforce § 512(h) subpoenas only in situations where they also had the right to demand that ISPs remove or disable access to infringing material stored on an ISP's network.

That reading of the statute is not only convoluted – it is palpably wrong. Indeed, it is contradicted by another provision in § 512(h) itself – § 512(h)(5) – which the D.C. Circuit ignored. As the United States has explained, "[b]y its

terms Section 512(h) provides that an ISP served with a subpoena 'shall expeditiously disclose * * * the information required by the subpoena, notwithstanding any other provision of law *and regardless of whether the service provider responds to the notification.*'" US Charter Br. at 23-24 (quoting 17 U.S.C. § 512(h)(5)) (emphasis and ellipses by United States). Congress thus stated quite plainly that an ISP must respond to a § 512(h) subpoena even if it believes it is under no duty to remove or disable access to infringing material pursuant to § 512(c) because the infringing material is not stored on its network. Moreover, the substantive limitation the D.C. Circuit derived from (c)(3)(A) appears nowhere in the text of that provision: subsection (c)(3)(A) does not specify that the infringing material must be on an ISP's network nor does it require the ISP to disable access to anything. *See* 17 U.S.C. § 512(c)(3)(A).

In all events, even if an ISP must be able to "disable access" to infringing material in order to come within the scope of § 512(h), the provision can be satisfied when an ISP subscriber stores infringing material on a home computer. As the United States has explained, "an ISP *can* deny access to infringing material that resides on a subscriber's computer, and hence a copyright owner *can* present a notification that conforms to the requirements of subsection (c)(3)(A)." US Charter Br. at 22 (emphasis in original). The D.C. Circuit believed that "Verizon can not remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers." Pet. App. 9a-10a. As a matter of plain English and common sense, however, an ISP can "disable access to [infringing material] simply by terminating or suspending the subscriber's Internet account, thereby preventing other peer-to-peer users from reaching

the infringing files." US Charter Br. at 23 (citing Pet. App. 33a n.5).[16]

Given that Congress took such care to define "service provider" in § 512, it strains credulity that Congress would have limited the scope of § 512(h) by the circuitous route of an oblique cross-reference to a notification provision in § 512(c)(3)(A), which in turn would have to be interpreted by reference to yet another provision, § 512(j).

Indeed, the D.C. Circuit's reading of § 512(h) is self-evidently antithetical to Congress' purpose, and thus conflicts with this Court's repeated admonition that an interpretation of a statutory text must be consistent with the statute's purpose. *See, e.g., General Dynamics Land Sys., Inc. v. Cline*, 124 S. Ct. 1236, 1245 (2004) (interpreting statutory provision "in light of the statute's manifest purpose"); *Allied-Bruce Terminix Cos. v. Dobson*, 513 U.S. 265, 274, 278 (1995) (rejecting interpretation that, "when viewed in terms of the statute's basic purpose, seems anomalous"); *Holloway v.*

---

[16] To reject this straightforward argument, the D.C. Circuit resorted to yet another part of § 512, subsection 512(j), in which Congress purportedly used the term "disable access" to mean something different from "terminating a subscriber's account." *See* Pet. App. 10a. The D.C. Circuit assumed that these terms must therefore be mutually exclusive. *Id.* But courts have routinely recognized that distinct statutory terms can have an overlapping or common meaning – a possibility that the D.C. Circuit did not even consider. *See, e.g., Natural Res. Def. Council, Inc. v. U.S. EPA*, 907 F.2d 1146, 1163 (D.C. Cir. 1990) (rejecting argument that terms cannot have overlapping meaning where Congress "d[id] not explicitly indicate that they are to be mutually exclusive"); *Carson Harbor Vill., Ltd. v. Unocal Corp.*, 270 F.3d 863, 882 (9th Cir. 2001) (concluding that "there is at least substantial overlap between" two terms and "reject[ing] the interpretation that the difference in the definitions requires us to . . . make the terms mutually exclusive"); *United States v. Hill*, 79 F.3d 1477, 1482-83 (6th Cir. 1996) (noting that two terms in the same provision "must have different meanings," but concluding nonetheless "that there is considerable overlap between the two terms").

United States, 526 U.S. 1, 9 (1999) (adopting interpretation of statutory language that served the purpose reflected by the statute as a whole, and rejecting interpretation that would contravene Congress' intent); *United States v. Morton*, 467 U.S. 822, 833 (1984) (stressing significance of "underlying purpose" in ascertaining plain meaning of statutory term); *FBI v. Abramson*, 456 U.S. 615, 625 (1982) (adopting interpretation of statutory language that "more accurately reflects the intention of Congress, is more consistent with the structure of the Act, and more fully serves the purposes of the statute"); *United States v. Bisceglia*, 420 U.S. 141, 150 (1975) (holding that courts should not interpret a statute to "frustrate" Congress' purpose "absent unambiguous directions from Congress").

Congress crafted § 512(h) broadly to serve a primary aim of the statute – to enable copyright owners to bring suit against direct infringers, rather than bringing derivative claims against ISPs. Applying § 512(h) to all ISP functions vindicates the purposes of § 512. As the district court held, there is "no sound reason" to deny copyright owners the ability to sue infringers directly when infringing material is stored on computers or servers that do not belong to an ISP.[17] Regardless of where the copyrighted material is stored, the harm to the copyright owner is the same (irreparable), the burden on the ISP to determine the identity of the infringer is the same (minimal), and the conduct of the subscriber is the same (unlawful).

---

[17] Indeed, copyright owners seeking a DMCA subpoena generally do not know where infringing material is stored – they can determine only the IP address of the infringer and, through that information, the ISP to which that address is assigned. *See* Pet. App. 35a.

C. The DMCA Expressly Addressed Piracy Over Conduit Facilities And The D.C. Circuit Effectively Repealed Congress' Solution.

The D.C. Circuit justified its result in part by claiming that Congress had "no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works," Pet. App. 14a, and thus had not drafted the DMCA to address the problem of Internet piracy over conduit facilities. That belief is wrong, as is the conclusion the Circuit drew from it – namely, that the issues in this case "must be addressed in the first instance by the Congress." Pet. App. 16a. The reality is that Congress already addressed this issue, as the DMCA's text and legislative history make perfectly clear.

The whole point of the DMCA was, as the United States has explained, "to deal with [the problem of Internet piracy] *in its entirety*." US Charter Br. at 14 (emphasis added). It was not, as the D.C. Circuit suggests, a statute designed to address, in narrow terms, those types of software then being used to infringe copyrights on the Internet. Rather, the DMCA was enacted to establish broad, enduring rules for the future, and thus to avoid the necessity of ongoing legislative revision. As one sponsor (Senator Leahy) explained, the DMCA "address[es] the needs of creators, consumers, and commerce in the digital age and well into the next century." Pet. App. 41a.

The Congress that enacted the DMCA was well aware that Internet piracy involving material stored on home computers and merely transmitted over ISP networks was an everyday occurrence. As the United States has explained, "[a]lthough Congress may not have foreseen the specific problem of illegal peer-to-peer file transfers, it manifestly did anticipate the general problem of which peer-to-peer transfers are simply one instance – the problem of online

copyright infringement in which an ISP serves only as a conduit." US Charter Br. at 13-14. Indeed, the DMCA provides for a limitation on liability for so-called conduit ISPs in § 512(a) – a limitation that would have had no purpose if Congress did not understand that ISPs often served as mere conduits for infringing material transmitted from one home computer to another. Moreover, as discussed above, *see supra* pp. 3-7, the legislative history conclusively establishes that Congress knew in 1998 that FTP sites and BBS services on home computers and electronic mail were engines of copyright piracy. The D.C. Circuit's blindness to this legislative record is inexplicable.

Ironically, the solution Congress enacted in the DMCA was *exactly* what the ISP community recommended to Congress as early as 1996 – when the problem of piracy involving material stored on home computers was already a well-recognized phenomenon. At a legislative hearing, the general counsel of one of the largest ISPs specifically proposed that ISPs should be required, "[i]n those cases where the allegedly infringing content is not on facilities controlled by the [ISP], . . . [to] take[] reasonable steps to assist the copyright owner in identifying the party that does control the hosting facility (upon receipt of a subpoena if necessary)." *NII Copyright Protection Act of 1995 (Part 2): Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 104th Cong. 261 (Feb. 7-8, 1996) (Stephen Heaton, General Counsel, Compuserve). That, of course, is precisely the obligation Congress imposed when it enacted § 512(h).

In sum, the notion, advanced by the D.C. Circuit, that Congress has primary authority in the area of copyright and thus that copyright owners must seek a remedy from Congress has no application here – Congress already legislated to address this problem. Rather than defer to

Congress' expertise in the area of copyright, the D.C. Circuit has overridden it.

D. Review Is Urgently Needed.

This Court should review this issue now, as the D.C. Circuit's decision is causing ongoing, irreparable harm to copyright holders. Infringement of the kind that prompted RIAA to serve the subpoenas at issue in this case occurs millions of times a day.

In the District of Columbia, the decision below has stripped copyright holders of a critical tool provided by Congress to enforce their intellectual property rights. The effect of the decision below is akin to declaring a statute unconstitutional because it has so constricted the subpoena provision as to make it practically meaningless and to completely thwart Congress' intent. Delay in the resolution of this issue may forever deprive those copyright holders of the ability to identify infringers, as ISPs have made clear that they do not retain the identifying information for very long.[18]

The D.C. Circuit's decision is reverberating far beyond the District of Columbia. The decision below has effectively stopped the issuance of DMCA subpoenas in the context of peer-to-peer copyright infringement. A critical aspect of § 512(h) is Congress' express and repeated direction that

---

[18] Prior to the D.C. Circuit's opinion, the music industry's efforts to enforce their rights against anonymous infringers by means of the DMCA subpoena provision were bearing fruit. According to one study, the number of Americans unlawfully downloading music files dropped by half in the six months after the industry began filing suits and before the D.C. Circuit's opinion. *See* Pew Internet & American Life Project, *The Impact of Recording Industry Suits Against Music File Swappers* (Jan. 2004), *available at* http://www.pewinternet.org/reports/pdfs/PIP_File_Swapping_Memo_0104.pdf.

clerks issue subpoenas expeditiously and ISPs respond expeditiously so that copyright owners can protect their rights. In the wake of the D.C. Circuit's opinion, however, court clerks are unsure whether they can issue such subpoenas, and ISPs have made clear that they will not comply with them.

Moreover, this important issue is likely to recur. Indeed, the issue already is recurring in other jurisdictions, including in courts in the Fourth and Eighth Circuits. This Court should not wait for those courts to rule. This case presents a straightforward question of statutory construction, applied to a narrow set of material facts that are essentially the same in every case. The Court already has the benefit of thorough discussions (reaching opposite conclusions) by the district court and the D.C. Circuit, and it can obtain the considered views of the United States and the Copyright Office.

Finally, resolution of this issue is of enormous importance to the administration of the federal courts. Stripped of the expeditious process Congress created in § 512(h), copyright owners are relegated to a much more cumbersome procedure – filing John Doe suits against unknown infringers. Pursuing such suits significantly delays copyright owners' ability to stop the irreparable harm they face. Copyright owners must obtain court permission before seeking prompt discovery, and face the risk that ISPs will purge the information needed to match IP addresses to subscriber identities. Such lawsuits also impose enormous burdens and costs on the federal courts that far exceed the DMCA subpoena process.

Even where DMCA subpoenas might be issued, the D.C. Circuit's ruling will prompt collateral litigation in every case seeking enforcement of a § 512(h) subpoena to determine where the infringing material at issue is stored. Copyright owners typically will not know whether infringing material

resides on a subscriber's home computer or an ISP server, and serious questions exist as to whether computers linked to ISPs via DSL or cable modem should be considered part of the ISP's network. With its emphasis on expedition and simplicity, Congress cannot possibly have intended that such collateral litigation be a prerequisite to enforcement of § 512(h) subpoenas.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

STANLEY PIERRE-LOUIS
LINDA J. ZIRKELBACH
RECORDING INDUSTRY
ASSOCIATION OF AMERICA, INC.
1330 Connecticut Avenue, NW
Suite 300
Washington, D.C. 20036
(202) 775-0101

DONALD B. VERRILLI, JR.
Counsel of Record
THOMAS J. PERRELLI
DEANNE E. MAYNARD
JARED O. FREEDMAN
JENNER & BLOCK LLP
601 Thirteenth Street, NW
Washington, D.C. 20005
(202) 639-6000

Counsel for Petitioner

May 24, 2004

Appendix A

United States Court of Appeals,
District of Columbia Circuit.

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., Appellee,
v.
VERIZON INTERNET SERVICES, INC., Appellant.

Nos. 03-7015 & 03-7053.

Argued Sept. 16, 2003.
Decided Dec. 19, 2003.

Before: GINSBURG, Chief Judge,and ROBERTS, Circuit Judge, and WILLIAMS, Senior Circuit Judge.

Opinion for the Court filed by Chief Judge GINSBURG.

GINSBURG, Chief Judge:

This case concerns the Recording Industry Association of America's use of the subpoena provision of the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), to identify internet users the RIAA believes are infringing the copyrights of its members. The RIAA served two subpoenas upon Verizon Internet Services in order to discover the names of two Verizon subscribers who appeared to be trading large numbers of .mp3 files of copyrighted music via "peer-to- peer" (P2P) file sharing programs, such as KaZaA. Verizon refused to comply with the subpoenas on various legal grounds.

The district court rejected Verizon's statutory and constitutional challenges to § 512(h) and ordered the internet

service provider (ISP) to disclose to the RIAA the names of the two subscribers. On appeal Verizon presents three alternative arguments for reversing the orders of the district court: (1) § 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others; if the statute does authorize such a subpoena, then the statute is unconstitutional because (2) the district court lacked Article III jurisdiction to issue a subpoena with no underlying "case or controversy" pending before the court; and (3) § 512(h) violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously. Because we agree with Verizon's interpretation of the statute, we reverse the orders of the district court enforcing the subpoenas and do not reach either of Verizon's constitutional arguments.[1]

I. Background

Individuals with a personal computer and access to the internet began to offer digital copies of recordings for download by other users, an activity known as file sharing, in the late 1990's using a program called Napster. Although recording companies and music publishers successfully obtained an injunction against Napster's facilitating the sharing of files containing copyrighted recordings, *see A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), millions of people in the United States and around the world continue to share digital .mp3 files of copyrighted

---

[1] The district court's jurisdiction to issue the orders here under review is not drawn into question by Verizon's Article III argument. *See Interstate Commerce Comm'n v. Brimson*, 154 U.S. 447, 476-78, 14 S. Ct. 1125, 1132-34, 38 L. Ed. 1047 (1894) (application of ICC to enforce subpoena issued by agency in furtherance of investigation presents "case or controversy" subject to judicial resolution).

recordings using P2P computer programs such as KaZaA, Morpheus, Grokster, and eDonkey. *See* John Borland, *File Swapping Shifts Up a Gear* (May 27, 2003), *available at* http://news.com.com/2100-1026-1009742.html, (last visited December 2, 2003). Unlike Napster, which relied upon a centralized communication architecture to identify the .mp3 files available for download, the current generation of P2P file sharing programs allow an internet user to search directly the .mp3 file libraries of other users; no web site is involved. *See* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J. LAW & TECH. 395, 403, 408-09 (2003). To date, owners of copyrights have not been able to stop the use of these decentralized programs. *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003) (holding Grokster not contributorily liable for copyright infringement by users of its P2P file sharing program).

The RIAA now has begun to direct its anti-infringement efforts against individual users of P2P file sharing programs. In order to pursue apparent infringers the RIAA needs to be able to identify the individuals who are sharing and trading files using P2P programs. The RIAA can readily obtain the screen name of an individual user, and using the Internet Protocol (IP) address associated with that screen name, can trace the user to his ISP. Only the ISP, however, can link the IP address used to access a P2P program with the name and address of a person - the ISP's customer - who can then be contacted or, if need be, sued by the RIAA.

The RIAA has used the subpoena provisions of § 512(h) of the Digital Millennium Copyright Act (DMCA) to compel ISPs to disclose the names of subscribers whom the RIAA has reason to believe are infringing its members' copyrights. *See* 17 U.S.C. § 512(h)(1) (copyright owner may "request the

clerk of any United States district court to issue a subpoena to [an ISP] for identification of an alleged infringer"). Some ISPs have complied with the RIAA's § 512(h) subpoenas and identified the names of the subscribers sought by the RIAA. The RIAA has sent letters to and filed lawsuits against several hundred such individuals, each of whom allegedly made available for download by other users hundreds or in some cases even thousands of .mp3 files of copyrighted recordings. Verizon refused to comply with and instead has challenged the validity of the two § 512(h) subpoenas it has received.

A copyright owner (or its agent, such as the RIAA) must file three items along with its request that the Clerk of a district court issue a subpoena: (1) a "notification of claimed infringement" identifying the copyrighted work(s) claimed to have been infringed and the infringing material or activity, and providing information reasonably sufficient for the ISP to locate the material, all as further specified in § 512(c)(3)(A); (2) the proposed subpoena directed to the ISP; and (3) a sworn declaration that the purpose of the subpoena is "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting" rights under the copyright laws of the United States. 17 U.S.C. §§ 512(h)(2)(A)-(C). If the copyright owner's request contains all three items, then the Clerk "shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the [ISP]." 17 U.S.C. § 512(h)(4). Upon receipt of the subpoena the ISP is "authorize[d] and order[ed]" to disclose to the copyright owner the identity of the alleged infringer. *See* 17 U.S.C. §§ 512(h)(3), (5).

On July 24, 2002 the RIAA served Verizon with a subpoena issued pursuant to § 512(h), seeking the identity of a subscriber whom the RIAA believed to be engaged in

infringing activity. The subpoena was for "information sufficient to identify the alleged infringer of the sound recordings described in the attached notification." The "notification of claimed infringement" identified the IP address of the subscriber and about 800 sound files he offered for trading; expressed the RIAA's "good faith belief" the file sharing activity of Verizon's subscriber constituted infringement of its members' copyrights; and asked for Verizon's "immediate assistance in stopping this unauthorized activity." "Specifically, we request that you remove or disable access to the infringing sound files via your system."

When Verizon refused to disclose the name of its subscriber, the RIAA filed a motion to compel production pursuant to Federal Rule of Civil Procedure 45(c)(2)(B) and § 512(h)(6) of the Act. In opposition to that motion, Verizon argued § 512(h) does not apply to an ISP acting merely as a conduit for an individual using a P2P file sharing program to exchange files. The district court rejected Verizon's argument based upon "the language and structure of the statute, as confirmed by the purpose and history of the legislation," and ordered Verizon to disclose to the RIAA the name of its subscriber. *In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24, 45 (D.D.C. 2003) (*Verizon I*).

The RIAA then obtained another § 512(h) subpoena directed to Verizon. This time Verizon moved to quash the subpoena, arguing that the district court, acting through the Clerk, lacked jurisdiction under Article III to issue the subpoena and in the alternative that § 512(h) violates the First Amendment. The district court rejected Verizon's constitutional arguments, denied the motion to quash, and again ordered Verizon to disclose the identity of its subscriber. *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 247, 275 (D.D.C. 2003) (*Verizon II*).

Verizon appealed both orders to this Court and we consolidated the two cases. As it did before the district court, the RIAA defends both the applicability of § 512(h) to an ISP acting as a conduit for P2P file sharing and the constitutionality of § 512(h). The United States has intervened solely to defend the constitutionality of the statute.

II. Analysis

The court ordinarily reviews a district court's grant of a motion to compel or denial of a motion to quash for abuse of discretion. *See, e.g., In re Sealed Case*, 121 F.3d 729, 740 (D.C. Cir. 1997). Here, however, Verizon contends the orders of the district court were based upon errors of law, specifically errors regarding the meaning of § 512(h). Our review is therefore plenary. *See In re Subpoena Served Upon the Comptroller of the Currency*, 967 F.2d 630, 633 (D.C. Cir. 1992).

The issue is whether § 512(h) applies to an ISP acting only as a conduit for data transferred between two internet users, such as persons sending and receiving e-mail or, as in this case, sharing P2P files. Verizon contends § 512(h) does not authorize the issuance of a subpoena to an ISP that transmits infringing material but does not store any such material on its servers. The RIAA argues § 512(h) on its face authorizes the issuance of a subpoena to an "[internet] service provider" without regard to whether the ISP is acting as a conduit for user-directed communications. We conclude from both the terms of § 512(h) and the overall structure of § 512 that, as Verizon contends, a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.

A. Subsection 512(h) by its Terms

We begin our analysis, as always, with the text of the statute. *See Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450, 122 S. Ct. 941, 950, 151 L. Ed. 2d 908 (2002). Verizon's statutory arguments address the meaning of and interaction between §§ 512(h) and 512(a)-(d). Having already discussed the general requirements of § 512(h), we now introduce §§ 512(a)-(d).

Section 512 creates four safe harbors, each of which immunizes ISPs from liability for copyright infringement under certain highly specified conditions. Subsection 512(a), entitled "Transitory digital network communications," provides a safe harbor "for infringement of copyright by reason of the [ISP's] transmitting, routing, or providing connections for" infringing material, subject to certain conditions, including that the transmission is initiated and directed by an internet user. *See* 17 U.S.C. §§ 512(a)(1)-(5). Subsection 512(b), "System caching," provides immunity from liability "for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the [ISP]," § 512(b)(1), as long as certain conditions regarding the transmission and retrieval of the material created by the ISP are met. *See* 17 U.S.C. §§ 512(b)(2)(A)-(E). Subsection 512(c), "Information residing on systems or networks at the direction of users," creates a safe harbor from liability "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider," as long as the ISP meets certain conditions regarding its lack of knowledge concerning, financial benefit from, and expeditious efforts to remove or deny access to, material that is infringing or that is claimed to be the subject of infringing activity. *See* 17 U.S.C. §§ 512(c)(1)(A)-(C).

Finally, § 512(d), "Information location tools," provides a safe harbor from liability "for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools" such as "a directory, index, reference, pointer, or hypertext link," subject to the same conditions as in §§ 512(c)(1)(A)-(C). *See* 17 U.S.C. §§ 512(d)(1)-(3).

Notably present in §§ 512(b)-(d), and notably absent from § 512(a), is the so-called notice and take-down provision. It makes a condition of the ISP's protection from liability for copyright infringement that "upon notification of claimed infringement as described in [§ 512](c)(3)," the ISP "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing." *See* 17 U.S.C. §§ 512(b)(2)(E), 512(c)(1)(C), and 512(d)(3).

Verizon argues that § 512(h) by its terms precludes the Clerk of Court from issuing a subpoena to an ISP acting as a conduit for P2P communications because a § 512(h) subpoena request cannot meet the requirement in § 512(h)(2)(A) that a proposed subpoena contain "a copy of a notification [of claimed infringement, as] described in [§ 512](c)(3)(A)."[2] In particular, Verizon maintains the two

---

[2] Subsection 512(c)(3)(A) provides that "[t]o be effective under this subsection, a notification of claimed infringement must be a written communication . . . that includes substantially the following":

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is

subpoenas obtained by the RIAA fail to meet the requirements of § 512(c)(3)(A)(iii) in that they do not - because Verizon is not storing the infringing material on its server - and can not, identify material "to be removed or access to which is to be disabled" by Verizon. Here Verizon points out that § 512(h)(4) makes satisfaction of the notification requirement of § 512(c)(3)(A) a condition precedent to issuance of a subpoena: "If the notification filed satisfies the provisions of [§ 512](c)(3)(A)" and the other content requirements of § 512(h)(2) are met, then "the clerk shall expeditiously issue and sign the proposed subpoena ... for delivery" to the ISP.

Infringing material obtained or distributed via P2P file sharing is located in the computer (or in an off-line storage device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the ISP can neither "remove" nor "disable access to" the infringing material because that material is not stored on the ISP's servers. Verizon can not remove or disable one user's access to infringing material resident on another user's

---

to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

17 U.S.C. § 512(c)(3)(A).

computer because Verizon does not control the content on its subscribers' computers.

The RIAA contends an ISP can indeed "disable access" to infringing material by terminating the offending subscriber's internet account. This argument is undone by the terms of the Act, however. As Verizon notes, the Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies for the protection of copyright owners, the former blocking access to the infringing material on the offender's computer and the latter more broadly blocking the offender's access to the internet (at least via his chosen ISP). *Compare* 17 U.S.C. § 512(j)(1)(A)(i) (authorizing injunction restraining ISP "from providing access to infringing material") *with* 17 U.S.C. § 512(j)(1)(A)(ii) (authorizing injunction restraining ISP "from providing access to a subscriber or account holder ... who is engaging in infringing activity ... by terminating the accounts of the subscriber or account holder"). "[W]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings." *Transbrasil S.A. Linhas Aereas v. Dep't of Transp.*, 791 F.2d 202, 205 (D.C. Cir. 1986). These distinct statutory remedies establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer.

The RIAA points out that even if, with respect to an ISP functioning as a conduit for user-directed communications, a copyright owner cannot satisfy the requirement of § 512(c)(3)(A)(iii) by identifying material to be removed by the ISP, a notification is effective under § 512(c)(3)(A) if it "includes substantially" the required information; that standard is satisfied, the RIAA maintains, because the ISP can identify the infringer based upon the information

provided by the copyright owner pursuant to §§ 512(c)(3)(A)(i) - (ii) and (iv)-(vi). According to the RIAA, the purpose of § 512(h) being to identify infringers, a notice should be deemed sufficient so long as the ISP can identify the infringer from the IP address in the subpoena.

Nothing in the Act itself says how we should determine whether a notification "includes substantially" all the required information; both the Senate and House Reports, however, state the term means only that "technical errors . . . such as misspelling a name" or "supplying an outdated area code" will not render ineffective an otherwise complete § 512(c)(3)(A) notification. S. Rep. No. 105-190, at 47 (1998); H.R. Rep. No. 105-551 (II), at 56 (1998). Clearly, however, the defect in the RIAA's notification is not a mere technical error; nor could it be thought "insubstantial" even under a more forgiving standard. The RIAA's notification identifies absolutely no material Verizon could remove or access to which it could disable, which indicates to us that § 512(c)(3)(A) concerns means of infringement other than P2P file sharing.

Finally, the RIAA argues the definition of "[internet] service provider" in § 512(k)(1)(B) makes § 512(h) applicable to an ISP regardless what function it performs with respect to infringing material - transmitting it per § 512(a), caching it per § 512(b), hosting it per § 512(c), or locating it per § 512(d).

This argument borders upon the silly. The details of this argument need not burden the Federal Reporter, for the specific provisions of § 512(h), which we have just rehearsed, make clear that however broadly "[internet] service provider" is defined in § 512(k)(1)(B), a subpoena may issue to an ISP only under the prescribed conditions regarding notification. Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the

copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A). And as we have seen, any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of § 512(c)(3)(A)(iii) and is therefore ineffective.

In sum, we agree with Verizon that § 512(h) does not by its terms authorize the subpoenas issued here. A § 512(h) subpoena simply cannot meet the notice requirement of § 512(c)(3)(A)(iii).

B. Structure

Verizon also argues the subpoena provision, § 512(h), relates uniquely to the safe harbor in § 512(c) for ISPs engaged in storing copyrighted material and does not apply to the transmitting function addressed by the safe harbor in § 512(a). Verizon's claim is based upon the "three separate cross - references" in § 512(h) to the notification described in § 512(c)(3)(A). First, as we have seen, § 512(h)(2)(A) requires the copyright owner to file, along with its request for a subpoena, the notification described in § 512(c)(3)(A). Second, and again as we have seen, § 512(h)(4) requires that the notification satisfy "the provisions of [§ 512](c)(3)(A)" as a condition precedent to the Clerk's issuing the requested subpoena. Third, § 512(h)(5) conditions the ISP's obligation to identify the alleged infringer upon "receipt of a notification described in [§ 512](c)(3)(A)." We agree that the presence in § 512(h) of three separate references to § 512(c) and the absence of any reference to § 512(a) suggests the subpoena power of § 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.

As the RIAA points out in response, however, because §§ 512(b) and (d) also require a copyright owner to provide a "notification . . . as described in [§ 512](c)(3)," the cross-

references to § 512(c)(3)(A) in § 512(h) can not confine the operation of § 512(h) solely to the functions described in § 512(c), but must also include, at a minimum, the functions described in §§ 512(b) and (d). Therefore, according to the RIAA, because Verizon is mistaken in stating that "the take-down notice described in [§ 512](c)(3)(A) . . . applies exclusively to the particular functions described in [§ 512](c) of the statute," the subpoena power in § 512(h) is not linked exclusively to § 512(c) but rather applies to all the ISP functions, wherever they may be described in §§ 512(a)-(d).

Although the RIAA's conclusion is a non-sequitur with respect to § 512(a), we agree with the RIAA that Verizon overreaches by claiming the notification described in § 512(c)(3)(A) applies only to the functions identified in § 512(c). As Verizon correctly notes, however, the ISP activities described in §§ 512(b) and (d) are storage functions. As such, they are, like the ISP activities described in § 512(c) and unlike the transmission functions listed in § 512(a), susceptible to the notice and take down regime of §§ 512(b)-(d), of which the subpoena power of § 512(h) is an integral part. We think it clear, therefore, that the cross-references to § 512(c)(3) in §§ 512(b)-(d) demonstrate that § 512(h) applies to an ISP storing infringing material on its servers in any capacity - whether as a temporary cache of a web page created by the ISP per § 512(b), as a web site stored on the ISP's server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d) - and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.

The storage activities described in the safe harbors of §§ 512(b)-(d) are subject to § 512(c)(3), including the notification described in § 512(c)(3)(A). By contrast, as we have already seen, an ISP performing a function described in § 512(a), such as transmitting e-mails, instant messages, or

files sent by an internet user from his computer to that of another internet user, cannot be sent an effective § 512(c)(3)(A) notification. Therefore, the references to § 512(c)(3) in §§ 512(b) and (d) lead inexorably to the conclusion that § 512(h) is structurally linked to the storage functions of an ISP and not to its transmission functions, such as those listed in § 512(a).

C. Legislative History

In support of its claim that § 512(h) can - and should - be read to reach P2P technology, the RIAA points to congressional testimony and news articles available to the Congress prior to passage of the DMCA. These sources document the threat to copyright owners posed by bulletin board services (BBSs) and file transfer protocol (FTP) sites, which the RIAA says were precursors to P2P programs.

We need not, however, resort to investigating what the 105th Congress may have known because the text of § 512(h) and the overall structure of § 512 clearly establish, as we have seen, that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others. Legislative history can serve to inform the court's reading of an otherwise ambiguous text; it cannot lead the court to contradict the legislation itself. *See Ratzlaf v. United States*, 510 U.S. 135, 147-48, 114 S. Ct. 655, 662-63, 126 L. Ed. 2d 615 (1994) ("[W]e do not resort to legislative history to cloud a statutory text that is clear").

In any event, not only is the statute clear (albeit complex), the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. That is not surprising; P2P software was "not even a glimmer in anyone's eye when the DMCA was enacted." *In*

re Verizon I, 240 F. Supp. 2d at 38. Furthermore, such testimony as was available to the Congress prior to passage of the DMCA concerned "hackers" who established unauthorized FTP or BBS sites on the servers of ISPs, *see Balance of Responsibilities on the Internet and the Online Copyright Liability Limitation Act: Hearing on H.R. 2180 Before the House Subcomm. on Courts and Intellectual Property, Comm. on the Judiciary*, 105th Cong. (1997) (statement of Ken Wasch, President, Software Publishers Ass'n); rogue ISPs that posted FTP sites on their servers, thereby making files of copyrighted musical works available for download, *see* Complaint, *Geffen Records, Inc. v. Arizona Bizness Network*, No. CIV. 98-0794, at ¶ 1 (D. Ariz. May 5, 1998) *available at* http://www.riaa.com/news/newsletter/pdf/geffencomplaint.pdf, (last visited December 2, 2003); and BBS subscribers using dial-up technology to connect to a BBS hosted by an ISP. The Congress had no reason to foresee the application of § 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along. Had the Congress been aware of P2P technology, or anticipated its development, § 512(h) might have been drafted more generally. Be that as it may, contrary to the RIAA's claim, nothing in the legislative history supports the issuance of a § 512(h) subpoena to an ISP acting as a conduit for P2P file sharing.

D. Purpose of the DMCA

Finally, the RIAA argues Verizon's interpretation of the statute "would defeat the core objectives" of the Act. More specifically, according to the RIAA there is no policy justification for limiting the reach of § 512(h) to situations in which the ISP stores infringing material on its system, considering that many more acts of copyright infringement are committed in the P2P realm, in which the ISP merely transmits the material for others, and that the burden upon

an ISP required to identify an infringing subscriber is minimal.

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." *See Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 431, 104 S. Ct. 774, 783, 78 L. Ed. 2d 574 (1984).

The stakes are large for the music, motion picture, and software industries and their role in fostering technological innovation and our popular culture. It is not surprising, therefore, that even as this case was being argued, committees of the Congress were considering how best to deal with the threat to copyrights posed by P2P file sharing schemes. *See, e.g., Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry: Hearing Before the Senate Comm. On Governmental Affairs*, 108th Congress (Sept. 30, 2003); *Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Comm. on the Judiciary*, 108th Congress (Sept. 9, 2003).

III. Conclusion

For the foregoing reasons, we remand this case to the district court to vacate its order enforcing the July 24 subpoena and to grant Verizon's motion to quash the February 4 subpoena.

So ordered.

Appendix B

United States District Court,
District of Columbia.

In re: VERIZON INTERNET SERVICES, INC.,
Subpoena Enforcement Matter,
Recording Industry Association of America, Plaintiff,
v.
Verizon Internet Services, Defendant.

No. CIV.A.02-MS-0323(JDB).

Jan. 21, 2003.

MEMORANDUM OPINION

BATES, District Judge.

The Recording Industry Association of America ("RIAA")[1] has moved to enforce a subpoena served on Verizon Internet Services ("Verizon") under the Digital Millennium Copyright Act of 1998 ("DMCA" or "Act"), 17 U.S.C. § 512. On behalf of copyright owners, RIAA seeks the identity of an anonymous user of Verizon's service who is alleged to have infringed copyrights with respect to more than 600 songs offered for downloading over the Internet in a single day. The copyright owners (and thus RIAA) can discern the Internet Protocol address, but not the identity, of the alleged infringer--only the service provider can identify the user. Verizon argues that the subpoena relates to

---

[1] RIAA is the industry trade association for sound and music recordings, whose members create and distribute the overwhelming majority of all music sold in the United States. RIAA is authorized to enforce the copyrights of its members.

material transmitted over Verizon's network, not stored on it, and thus falls outside the scope of the subpoena power authorized in the DMCA. RIAA counters that the subpoena power under section 512(h) of the DMCA applies to all Internet service providers, including Verizon, whether the infringing material is stored on or simply transmitted over the service provider's network.

The case thus presents a core issue of statutory interpretation relating to the scope of the subpoena authority under the DMCA. The parties, and several *amici curiae*, agree that this is an issue of first impression of great importance to the application of copyright law to the Internet. Indeed, they concede that this case is presented as a test case on the DMCA subpoena power. Based on the language and structure of the statute, as confirmed by the purpose and history of the legislation, the Court concludes that the subpoena power in 17 U.S.C. § 512(h) applies to all Internet service providers within the scope of the DMCA, not just to those service providers storing information on a system or network at the direction of a user. Therefore, the Court grants RIAA's motion to enforce, and orders Verizon to comply with the properly issued and supported subpoena from RIAA seeking the identity of the alleged infringer.

BACKGROUND

An assessment of this issue requires some understanding of both the DMCA and the subpoena served by RIAA on Verizon. Although the subpoena power is specifically delineated in section 512(h), that language cannot be isolated from the structure and purpose of the DMCA, and RIAA's subpoena to Verizon must be assessed in that context.

1. The Digital Millennium Copyright Act

The DMCA amended chapter 5 of the Copyright Act, 17 U.S.C. § 501 *et seq.*, and created a new section 512 entitled

"Limitations on liability relating to material online." As the title indicates, the DMCA is designed primarily to limit the liability of Internet service providers for acts of copyright infringement by customers who are using the providers' systems or networks. Section 512 contains limitations on the liability of service providers for four general categories of activity set forth in subsections (a) through (d). The statute thereby creates a series of "safe harbors" that allow service providers to limit their liability for copyright infringement by users if certain conditions under the Act are satisfied. "The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory [copyright] infringement." S. Rep. No. 105-190, at 20 (1998).

Under the DMCA, an Internet service provider falls within one of these four subsections based on how the allegedly infringing material has interacted with the service provider's system or network. To qualify for a "safe harbor," the service provider must fulfill the conditions under the applicable subsection and the conditions of subsection (*i*), which includes the requirement that a service provider implement and inform its users of its policy to terminate a subscriber's account in cases of repeat copyright infringement. *See* 17 U.S.C. § 512(*i*)(1)(A). Under subsection (a), which Verizon contends is applicable here, if the service provider meets certain conditions it will not be liable for the user's copyright infringement when the service provider transmits the copyrighted material over its system or network:

> (a) Transitory digital network communications.--A service provider shall not be liable . . . for infringement of copyright by reason of the provider's transmitting, routing, or providing [Internet] connections for, material through a

> system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections . . ..

Id. § 512(a). On the other hand, subsection (c), the other subsection most relevant here, pertains to copyrighted material that is **stored** on the service provider's network or system:

> (c) Information residing on systems or networks at direction of users. -- . . . A service provider shall not be liable . . . for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider . . ..

Id. § 512(c)(1).[2] Under subsection (c), a service provider must also designate an agent to receive notifications of claimed infringement from copyright owners. *Id.* § 512(c)(2).

Of particular importance here, subsection (c)(3)(A) spells out requirements to be met by copyright owners for effective notification of copyright infringement under subsection (c). The notification of claimed infringement must be in a writing provided to the designated agent, and must include the following -- a "signature of a person authorized to act on behalf of the [copyright] owner"; identification of the copyrighted work allegedly infringed (or a list of multiple

---

[2] Subsection (b) covers "system caching," which is the temporary storage of allegedly infringing material on the provider's system or network, while subsection (d) relates to "information location tools," which refer or link users to an online location having infringing material through the use of "a directory, index, reference, pointer, [ ] hypertext link" or other information location tool. *Id.* §§ 512(b) & (d).

copyrighted works covered by a single notification); identification of the allegedly infringing material "that is to be removed or access to which is to be disabled," and information to enable the provider to locate the material; information to permit the provider to contact the complaining party; a statement of good faith belief that the use complained of is not authorized; and a "statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner." *Id.* § 512(c)(3)(A)(i)-(vi). This notification requirement is located within subsection (c), and there is no similar notification requirement within subsection (a) or elsewhere in section 512. The subsection (c)(3) notification requirement is referenced, however, in the conditions under both subsection (b) and subsection (d). *See id.* §§ 512(b)(2)(E) & (d)(3).

The DMCA also contains a novel provision in subsection (h) -- which lies at the heart of the dispute before the Court -- permitting a copyright owner to obtain and serve a subpoena on a service provider seeking the identity of a customer alleged to be infringing the owner's copyright. The subpoena is issued by the clerk of any United States District Court upon a request by the copyright owner (or one authorized to act on the owner's behalf) containing the proposed subpoena, "a copy of a notification described in subsection (c)(3)(A)," and a sworn declaration ensuring that the subpoena is solely to obtain the identity of the alleged infringer, which information will be used only to protect rights to the copyright. *Id.* § 512(h)(2). The subpoena, in turn, authorizes and orders the recipient service provider "to expeditiously disclose" information sufficient to identify the alleged infringer. *Id.* § 512(h)(3). The clerk "shall expeditiously issue" the subpoena if it is in proper form, the declaration is properly executed, and "the notification filed satisfies the provisions of subsection (c)(3)(A)." *Id.* §

512(h)(4). The service provider, upon receipt of the subpoena, "shall expeditiously disclose" the information required by the subpoena to the copyright owner (or authorized person). *Id.* § 512(h)(5). The issuance, delivery and enforcement of subpoenas is to be governed (to the extent practicable) by the provisions of the Federal Rules of Civil Procedure dealing with subpoenas duces tecum. *Id.* § 512(h)(6).

2. RIAA's Subpoena to Verizon

On July 24, 2002, RIAA served a subpoena on Verizon seeking identifying information about an anonymous copyright infringer allegedly using Verizon's network to offer for downloading copyrighted songs through peer-to-peer software provided by KaZaA, without the copyright holders' authorization. *See* Motion to Enforce, Ex. A. Along with the subpoena, RIAA provided Verizon with a list of more than 600 files (predominantly individual songs, most by well-known artists) allegedly offered for downloading by the user on one day. *Id.*, Ex. B. The subpoena included the user's specified Internet Protocol (IP) address, to enable Verizon to locate the computer where the infringement occurred. In addition to the IP address, RIAA provided the time and date when the songs were downloaded and furnished a declaration, under penalty of perjury, that the information was sought in good faith and would only be used in connection with "protecting the rights" of RIAA members. *Id.*, Ex. B (letter from Whitehead to Crowder dated July 24, 2002). RIAA also requested that Verizon "remove or disable access to the infringing sound files." *Id.*

Verizon responded by letter refusing to comply with RIAA's subpoena. *Id.*, Ex. D (letter from Daily to Whitehead dated Aug. 6, 2002). Verizon emphasized its view that the DMCA subpoena power applies only if the infringed material is stored or controlled on the service provider's

system or network under subsection (c). *Id.* at pp. 2-3. Verizon stated: "The allegedly infringing contents of the [downloaded files] do not reside on any system or network controlled or operated by or for [Verizon], but . . . are stored on the hardware of the Customer. Thus, neither § 512(c)(3)(A) nor § 512(h) is applicable for this reason alone." *Id.* According to Verizon, a subpoena under the DMCA is "conditioned" on notification under section 512(c)(3)(A), "and that provision is addressed to 'material that resides on a system or network *controlled or operated by or for [a] service provider.*'" *Id.* (emphasis in original). In contrast, Verizon stressed, it only provided the customer with Internet connectivity service. *Id.* Verizon also refused RIAA's request to terminate the user's Internet connection. *Id.* at 3. Verizon's position, therefore, is that because it only provided the alleged infringer with an Internet connection, it falls under subsection (a) of section 512, not under subsection (c), and it is thus outside the subpoena authority of subsection (h), which Verizon contends is limited to service providers storing material under subsection (c).

RIAA, on the other hand, is of the view that the DMCA subpoena power under section 512(h) applies to all service providers within the provisions of subsections (a) through (d), including Verizon in the instant case.[3] Given Verizon's refusal to comply with the subpoena, RIAA moved pursuant to 17 U.S.C. § 512(h)(6) and Fed. R. Civ. P. 45(c)(2)(B) to enforce the subpoena. Substantial briefing (including submissions by *amici curiae* on both sides) and a hearing followed.

---

[3] Hence, RIAA submits that it does not matter for purposes of enforcement of the subpoena whether Verizon comes within subsection (a) or subsection (c) in this case; in either event, RIAA contends, the subpoena is valid.

ANALYSIS

This case turns on the meaning and scope of the provisions of the DMCA. "As in all statutory construction cases, we begin with the language of the statute." *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450, 122 S. Ct. 941, 151 L. Ed. 2d 908 (2002); *see also United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1352 (D.C. Cir. 2002). The first step "is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340, 117 S. Ct. 843, 136 L. Ed. 2d 808 (1997) (citing *United States v. Ron Pair Enters., Inc.*, 489 U.S. 235, 240, 109 S. Ct. 1026, 103 L. Ed. 2d 290 (1989)). If so, and if the statutory scheme is "coherent and consistent," then the inquiry ceases. *Barnhart*, 534 U.S. at 450, 122 S. Ct. 941 (quoting *Robinson*, 519 U.S. at 340, 117 S. Ct. 843). Nonetheless, "[s]tatutory construction 'is a holistic endeavor,' and, at a minimum, must account for a statute's full text, language as well as punctuation, structure, and subject matter." *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 254, 112 S. Ct. 1146, 117 L. Ed. 2d 391 (1992) (quoting *United Savings Ass'n of Texas v. Timbers of Inwood Forest Assocs., Ltd.*, 484 U.S. 365, 371, 108 S. Ct. 626, 98 L. Ed. 2d 740 (1988)). Hence, "courts should disfavor interpretations of statutes that render language superfluous." *Connecticut Nat'l Bank*, 503 U.S. at 253, 112 S. Ct. 1146. But as the Supreme Court has explained:

> [C]anons of construction are no more than rules of thumb that help courts determine the meaning of legislation, and in interpreting a statute a court should always turn first to one, cardinal canon before all others. We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.

Id. at 254, 112 S. Ct. 1146; *accord Ron Pair Enters., Inc.*, 489 U.S. at 241-42, 109 S. Ct. 1026; *United States v. Goldenberg*, 168 U.S. 95, 102-03, 18 S. Ct. 3, 42 L. Ed. 394 (1897). "When the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'" *Connecticut Nat'l Bank*, 503 U.S. at 254, 112 S. Ct. 1146 (quoting *Rubin v. United States*, 449 U.S. 424, 430, 101 S. Ct. 698, 66 L. Ed. 2d 633 (1981)); *see also Ratzlaf v. United States*, 510 U.S. 135, 147-48, 114 S. Ct. 655, 126 L. Ed. 2d 615 (1994) ("There are, we recognize, contrary indications in the statute's legislative history. But we do not resort to legislative history to cloud a statutory text that is clear."); *Barnhill v. Johnson*, 503 U.S. 393, 401, 112 S. Ct. 1386, 118 L. Ed. 2d 39 (1992).

Here, the statutory language and structure lead to a single result -- the section 512(h) subpoena authority applies to service providers within not only subsection (c) but also subsections (a), (b), and (d) of section 512. Moreover, the purpose and history of the DMCA are consistent with that conclusion.

1. Statutory Definition of "Service Provider"

The statutory text of the DMCA provides clear guidance for construing the subpoena authority of subsection (h) to apply to all service providers under the Act. The term "service provider" is employed repeatedly in subsection (h). The request to the clerk is "to issue a subpoena to a service provider for identification of an alleged infringer" (§ 512(h)(1)); the subpoena "shall authorize and order the service provider receiving the notification and the subpoena" to disclose the identifying information to the extent it is available to the service provider (§ 512(h)(3)); a proper subpoena shall be executed by the clerk, who shall return it to the requester "for delivery to the service provider" (§ 512(h)(4)); and upon receipt "the service provider shall expeditiously disclose" the information

required by the subpoena "regardless of whether the service provider responds to the notification" (§ 512(h)(5)).

The question, then, is whether the "service provider" repeatedly referenced in subsection (h) is limited to one described by subsection (c) or instead includes those described in subsections (a), (b) and (d) of section 512 as well. The DMCA answers that question unequivocally.

The Act provides two distinct definitions of "service provider" -- a narrow definition as the term is used solely within subsection (a), and a broader definition governing all other subsections, which specifically includes a "service provider" under subsection (a) as well:

> (k) Definitions. -
>
> (1) Service provider. -
>
> (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
>
> (B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

17 U.S.C. § 512(k); *see also ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 623 (4th Cir. 2001) (the DMCA "defines a service provider broadly").

The textual definition of "service provider" in subsection (k) leaves no doubt, therefore, that the subpoena power in subsection (h) applies to all service providers, regardless of the functions a service provider may perform under the four categories set out in subsections (a) through (d). The broad definition in subsection (k)(1)(B) -- "a provider of online services or network access" -- expressly applies to the term "service provider" as used in subsection (h), since the narrow definition found in subsection (k)(1)(A) is applicable only to the term as used in subsection (a). By the plain text of the statute, moreover, the term "service provider" as employed in subsection (h) encompasses those entities defined in subsection (k)(1)(A), which explicitly includes "service providers" under subsection (a) such as Verizon (an "entity offering the transmission, routing, or providing of connections for digital online communications"). In short, Verizon contends that it has only provided an Internet connection, and thus is within subsection (a) of the DMCA; but the definition of "service provider" in subsection (k) applicable to the subpoena authority under subsection (h) squarely includes subsection (a) entities such as Verizon that are "providing . . . connections for digital online communications." Given the broad definition of "service provider" in subsection (k)(1)(B), and the use of that defined term throughout subsection (h), the Court must, under well-established statutory construction tools, read these provisions together, as a whole. *See United States v. Wilson*, 290 F.3d 347, 355 (D.C. Cir. 2002) ("It is the 'classic judicial task' of construing related statutory provisions 'to make sense in combination.'") (quoting *United States v. Fausto*, 484 U.S. 439, 453, 108 S. Ct. 668, 98 L. Ed. 2d 830 (1988)). Applying the statutory definition of "service provider" leaves no doubt whatsoever, then, that the DMCA subpoena

authority reaches a subsection (a) service provider such as Verizon contends it is here.[4]

Verizon's response is to downplay the subsection (k) definition, dismissing it as "beside the point." But the language is clear, and the Court cannot overlook the governing definition of service provider in subsection (k)(1)(B), which plainly sets the scope of the subsection (h) subpoena power. Rather, the Court must take into account all relevant parts of the statute. *See United States Telecom Ass'n v. FCC*, 227 F.3d 450, 463 (D.C. Cir. 2000) (noting "the well-accepted principle of statutory construction that requires every provision of a statute to be given effect"); *Qi-Zhuo v. Meissner*, 70 F.3d 136, 139 (D.C. Cir. 1995) (courts have "endlessly reiterated [the] principle of statutory construction . . . that all words in a statute are to be assigned meaning, and that nothing therein is to be construed as surplusage"). "If a statute defines a term in its definitional section, then that definition controls the meaning of the term wherever it appears in the statute." *Lilly v. Internal Revenue Service*, 76 F.3d 568, 571 (4th Cir. 1996); *see also Colautti v. Franklin*, 439 U.S. 379, 392 n. 10, 99 S. Ct. 675, 58 L. Ed. 2d 596 (1979) ("[A] definition which declares what a term 'means' . . . excludes any meaning that is not stated."); *Florida Dep't of Banking & Fin. v. Board of Governors of Fed. Reserve Sys.*, 800

---

[4] The legislative history of the DMCA comports with this reading of the definitional language of subsection (k). The Senate Report explains that "[t]he second definition of 'service provider,' set forth in subsection (j)(1)(b), applies to the term as used in any other subsection of section 512." S. Rep. No. 105-190, at 54 (subsection (j)(1)(b) ultimately became subsection (k)(1)(B)). "This definition includes, for example, services such as providing Internet access, e-mail, chat room and web page hosting services," and "[t]he definition also specifically includes any entity that falls within the first definition of service provider." Id. at 54-55. See also H.R. Rep. No. 105-551(II), at 64 (1998) (definition of "service provider" "includes, for example, services such as providing Internet access, email," etc.).

F.2d 1534, 1536 (11th Cir. 1986) ("It is an elementary precept of statutory construction that the definition of a term in the definitional section of a statute controls the construction of that term wherever it appears throughout the statute."). It would simply make no sense here to dismiss the statutory definition of "service provider" as irrelevant.

As Verizon explained in its letter to RIAA refusing to comply with the subpoena, "the only service [Verizon] provides to the Customer is Internet connectivity." Motion to Enforce, Ex. D, at p. 2 (letter from Dailey to Whitehead dated Aug. 6, 2002). But the broad definition of "service provider" under subsection (k)(1)(B) that is expressly applicable to subsection (h), together with the fact that Verizon indisputably provided network access to the alleged infringer, lead ineluctably to the conclusion that the subpoena authority of the DMCA applies to all service providers within the scope of the Act, including those like Verizon falling under subsection (a).

2. The Statutory Structure

Verizon's assertions to the contrary are refuted by the structure and language of the DMCA. An essential condition for a valid subpoena under subsection 512(h), Verizon claims, "is a notification to the service provider that complies with subsection (c)(3)(A)." Verizon Opp. at pp. 2-3. Therefore, Verizon argues, it is implicit that a subpoena may only be issued to service providers described in subsection (c) -- in other words, "to [those] service providers who have stored offending material on their own system or network." *Id.* at p. 3. Verizon notes that, in contrast, "subsection (a) -- the provision of section 512 for service providers acting simply as passive transmitters, as Verizon was here -- contains no provision for any notification of claimed infringers, much less notification that 'satisfies the requirements of (c)(3)(A).'" *Id.* Thus, Verizon reasons,

RIAA's subpoena to it is invalid because Verizon is not storing the infringing material on its system or network, but is simply providing "Internet connectivity" or acting as a "passive conduit" under subsection (a), and hence need not comply with the notification requirement in subsection (c)(3)(A).

The Court disagrees with Verizon's strained reading of the Act, which disregards entirely the clear definitional language of subsection (k). The holistic character of statutory construction requires an examination of all relevant text, and of language as well as structure. *See Connecticut Nat'l Bank*, 503 U.S. at 254, 112 S. Ct. 1146. Not only the language but also the structure of the DMCA dispenses with the contentions advanced by Verizon.

Verizon contends that the Court should infer that the subpoena authority under subsection (h) only applies to subsection (c) in light of the reference in subsection (h)(2)(A) to the notification requirement of subsection (c)(3)(A). But that reference does not mean that subsection (h) only applies to service providers described in subsection (c). In fact, the notification provision in subsection (c) is also referenced elsewhere in the DMCA, including in subsections (b)(2)(E) and (d)(3). The latter references confirm the expectation that notifications like that described in subsection (c)(3) will at times be needed in settings under subsections (b) and (d), and hence are not confined to subsection (c) settings. Subsection (h), moreover, is written without limitation or restriction as to its application. It is entitled "Subpoena to identify infringer" – not "Subpoena to identify infringer storing copyrighted material on a service provider's network" or "Subpoena to identify infringer relating to subsection (c)" If Congress intended to restrict or limit the subsection (h) subpoena authority based on where the infringing material resides, one would expect to see that

limitation spelled out in subsection (h). And if Congress intended to limit subsection (h) subpoenas strictly to service providers under subsection (c), it certainly could have made such a limitation explicit.

There is simply nothing in the text of the statute that states, or even suggests, that the subpoena authority in subsection (h) applies only to those service providers described in subsection (c). Indeed, subsection (h) does not require, as Verizon contends, a copyright owner to comply fully with subsection (c)(3)(A). The references in subsection (h) to "a notification described in" (*see* §§ 512(h)(2)(A) & (h)(5)) or that "satisfies the provisions of" (*see* § 512(h)(4)) subsection (c)(3)(A) do not by their language limit the subpoena authority. Rather, these references are consistent with the construction that when a subpoena under subsection (h) is sought against a service provider falling within subsections (a), (b) or (d), the copyright owner or authorized person must then provide a notification like the one always required under subsection (c) but not otherwise required under (a), (b) or (d). Thus, as part of the process to obtain a subpoena, subsection (h)(2)(A) simply requires a copyright owner to file with the clerk the type of "notification described in subsection (c)(3)(A)."

Significantly, then, if Congress had intended subsection (h) subpoenas to apply solely to subsection (c) service providers, it could have stated such a limitation in subsection (h), or stated that subsection (h) does not apply to subsections (a), (b) or (d), or even have placed the subpoena authority itself within subsection (c). But Congress did not do so. Instead, the subpoena authority in the DMCA is contained in a stand-alone subsection, just as separate from

subsection (c) as it is from subsections (a), (b), and (d).[5] It is a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133, 120 S. Ct. 1291, 146 L. Ed. 2d 121 (2000).

Verizon's proposed construction does not comport with other aspects of the Act either. A court must consider "the particular statutory language at issue, as well as the

---

[5] Verizon also points out that under subsection (c)(3)(A)(iii) a copyright owner must identify the infringing material "that is to be removed or access to which is to be disabled." In order to remove or disable access to the material, Verizon argues, the material must be stored on its system -- an indication that Congress intended subsection (h) to apply only to those service providers who store infringing material on their systems. The Court is not persuaded. To begin with, a subpoena issued pursuant to subsection (h) is used to identify the infringer, not to force the service provider to remove material or disable access to it. The requirement for the notification is simply that it identify the infringing material to be removed, not that removal be effectuated. In addition, a copyright owner can meet the requirement under subsection (c)(3)(A)(iii) if it can disable access to material. Here, Verizon certainly can disable access to the material by terminating the account altogether. Verizon makes clear to customers in its terms of service that the use of its network for copyright infringement is strictly forbidden, and can result in a variety of sanctions, including termination. In fact, the DMCA *requires* service providers, in order to obtain the various safe harbor protections, to implement "a policy that provides for termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." 17 U.S.C. § 512(*i*) (1)(A). Verizon counters that terminating service is too harsh, and may prevent other family members from having Internet service. But again, the requirement is only identification of infringing material, not actual removal or access denial. There is nothing, moreover, to prevent a family member from opening another account. In any event, it is irrelevant whether the service provider is able, or intends, to disable access to the material. *See id.* § 512(h)(5) ("service provider shall expeditiously disclose to the copyright owner . . . the information required by the subpoena, . . . regardless of whether the service provider responds to the notification").

language and design of the statute as a whole." *K Mart v. Cartier, Inc.*, 486 U.S. 281, 291, 108 S. Ct. 1811, 100 L. Ed. 2d 313 (1988). There is no discernable reason why Congress would limit the subpoena authority under subsection (h) to subsection (c) service providers alone. To begin with, the burden on a service provider in identifying an apparent infringer is no different depending on which subsection of 512 is implicated.[6] Indeed, considering the four-part structure of the liability limitations under the DMCA, subsections (a) through (d) together with the subpoena authority under subsection (h) only "make sense in combination" if construed so that the subpoena authority extends to service providers in all four categories. *See Fausto*, 484 U.S. at 453, 108 S. Ct. 668; *Wilson*, 290 F.3d at 355. Otherwise, the statute would fail significantly to address many contexts in which a copyright owner needs to utilize the subpoena process in order to discern the identity of an apparent copyright infringer. And although Verizon has attempted to justify an exclusion of just subsection (a) service providers from the reach of the subpoena authority, the position advanced by Verizon logically supports confining the subpoena authority to subsection (c) service providers alone, whereas the statutory language and structure certainly provide no basis for differentiating service providers within subsection (a) from those within subsections (b) and (d) as to the scope of the subpoena power. Moreover, whatever rationale warrants

---

[6] Arguably, the total burden on service providers may be heavier from subpoenas relating to subsection (a), as there may be more infringement occurring with subsection (a) service providers than with subsection (c) service providers. But in exchange for complying with subpoenas under subsection (h), service providers receive liability protection from any copyright infringement -- direct or vicarious -- by their users. Hence, any additional burden is offset by that protection, which, of course, is exactly the contemplation reflected in the structure of the DMCA.

distinguishing among subsections (a) through (d) for purposes of the safe harbor liability protections, there is no corresponding rationale for such distinctions regarding a subpoena power that entails merely identifying infringers.

Importantly, Verizon's construction does not square with Congress's express and repeated direction to make the subpoena process "expeditious." *See, e.g.*, 17 U.S.C. §§ 512(h)(3), (h)(4) & (h)(5) (subpoena shall require service provider to expeditiously disclose identity of infringer; clerk shall expeditiously issue subpoena; and service provider shall expeditiously disclose identity of infringer upon receipt of subpoena). The statute contemplates a rapid subpoena process designed quickly to identify apparent infringers and then curtail the infringement. The copyright holder, however, cannot readily determine whether its infringed material was stored on or merely transmitted across the service provider's system, and hence whether it faces a subsection (c) or subsection (a) situation. As a result, if the copyright owner could only utilize the subpoena process for subsection (c) service providers, it would have to establish at the outset that the service provider fell within subsection (c) in the particular case at hand. Hence, in many instances an initial contested factual issue would ensue in court with respect to where the material is stored, resulting in potentially lengthy delays in obtaining identifying information about the infringer. Such complication and delay hardly comports with the language peppered throughout subsection (h) indicating that the subpoena process should be "expeditious." In fact, there is an important reason why Congress required service providers to act promptly upon receipt of a subpoena to prevent further infringement -- "the ease with which digital works

can be copied and distributed worldwide virtually instantaneously." S. Rep. No. 105-190, at 8.[7]

Verizon's construction thus makes little sense from a policy standpoint. Verizon has provided no sound reason why Congress would enable a copyright owner to obtain identifying information from a service provider storing the infringing material on its system, but would not enable a copyright owner to obtain identifying information from a service provider transmitting the material over its system (or, indeed, from a service provider engaged in system caching under subsection (b) or providing information location tools under subsection (d)). After all, the information obtained simply permits the copyright owner to take steps directly with the infringer to prevent further infringement. It is unlikely, the Court concludes, that Congress would seek to protect copyright owners in only some of the settings addressed in the DMCA, but not in others.

In short, Verizon's position that the subpoena power in subsection (h) only applies to subsection (c) service providers, and not to subsection (a) (or for that matter to subsections (b) and (d)) service providers, would create a huge loophole in Congress's effort to prevent copyright infringement on the Internet. There is little doubt that the largest opportunity for copyright theft is through peer-to-peer ("P2P") software, as used by the alleged infringer here.

---

[7] The consequence of delaying the receipt of information identifying an infringer was highlighted by *amicus curiae* Motion Picture Association of America. If Warner Brothers sought to obtain by subpoena information identifying an alleged infringer disseminating the latest Warner Brothers' movie release over the Internet, but needed first to establish that the movie was stored on the service provider's system, the movie could be distributed all over the world in the meantime, dramatically diminishing the value of the copyright.

One *amici* characterizes such P2P software as "the biggest revolution to happen on the Internet since the advent of email or the World Wide Web -- millions of individuals use P2P now, and the number is growing exponentially." Br. of *Amicus Curiae* U.S. Internet Service Provider Assoc. at p. 6. Even Verizon states that "more than 100 million copies of [KaZaA's] peer-to-peer file sharing software have been downloaded, and more than two million of its users are commonly online at any given time." Verizon Opp. at p. 8. Because peer-to-peer users most often swap materials over the Internet that are stored on their own computers -- not on the service providers' networks -- such activity is within subsection (a), not subsection (c). Thus, under Verizon's reading of the Act, a significant amount of potential copyright infringement would be shielded from the subpoena authority of the DMCA.[8] That would, in effect, give Internet copyright infringers shelter from the long arm of the DMCA subpoena power, and allow infringement to flourish. The Court can find nothing in the language or structure of the statute that suggests Congress intended the DMCA to protect only a very limited portion of copyrighted material on the Internet.

3. The Purpose and History of the DMCA

"The traditional tools [of statutory construction] include examination of the statute's text, legislative history, and

---

[8] Verizon recognizes the extent of this resulting loophole. In addressing the burden on service providers if subsection (h) applied to subsection (a), Verizon conceded at oral argument that far more infringement occurs with subsection (a) service providers: "There are, under subsection (a), far greater number of uses, e-mail, for instance, is part of subsection (a). The whole Internet is potentially drawn into subsection (a)." Tr. of Hearing (Oct. 4, 2002) at p. 61. Indeed, as one District Court observed in construing an unrelated provision of the DMCA, "piracy of intellectual property has reached epidemic proportions." *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1132 (N.D. Cal. 2002).

structure, as well as its purpose." *Natural Resources Defense Council, Inc., v. Daley*, 209 F.3d 747, 752 (D.C. Cir. 2000). Here, the text and structure of the DMCA are clear, as explained above, and "we do not resort to legislative history to cloud a statutory text that is clear." *Ratzlaf v. United States*, 510 U.S. at 147- 48, 114 S. Ct. 655. Nonetheless, common sense suggests that an assessment of the subpoena authority under the DMCA may benefit from an understanding of the purpose and history of the legislation. *See Wisconsin Public Intervenor v. Mortier*, 501 U.S. 597, 611 n. 4, 111 S. Ct. 2476, 115 L. Ed. 2d 532 (1991).

Congress not only sought to limit the liability of service providers under the DMCA, but also intended to assist copyright owners in protecting their copyrights. The legislative history makes clear that in enacting the DMCA, Congress attempted to balance the liability protections for service providers with the need for broad protection of copyrights on the Internet.[9] The clear purpose of the DMCA, evident in its legislative history, confirms that the scope of the subsection (h) subpoena power extends to service providers within subsection (a) as well as subsection (c).

The dual purpose and balance of the DMCA has been recognized by the courts. The Fourth Circuit has explained that "[t]he DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider."

---

[9] To the extent the statutory language in the DMCA is unclear, "the legislative history of the DMCA can be useful in fleshing out its meaning given the paucity of precedent interpreting the statute." *Costar Group, Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688, 700 (D. Md. 2001).

ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001). Other courts note this balancing as well. "Congress was concerned with promoting electronic commerce while protecting the rights of copyright owners, particularly in the digital age where near exact copies of protected works can be made at virtually no cost and distributed instantaneously on a worldwide basis." *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1124 (N.D. Cal. 2002) (citing S. Rep. No. 105-190, at 8). In short, Congress sought "to protect against unlawful piracy and promote the development of electronic commerce and the availability of copyrighted material on the Internet." *Id.* at 1125.

Congress thus created tradeoffs within the DMCA: service providers would receive liability protections in exchange for assisting copyright owners in identifying and dealing with infringers who misuse the service providers' systems. At the same time, copyright owners would forgo pursuing service providers for the copyright infringement of their users, in exchange for assistance in identifying and acting against those infringers.

> Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.

S. Rep. No. 105-190, at 20. "[T]he Committee believes it has appropriately balanced the interests of content owners, on-line and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the Internet." H.R. Rep. No.

105- 551(II), at 21; *see also* H.R. Rep. No. 105-551(I), at 11 (noting that remedies "ensur[e] that it is possible for copyright owners to secure the cooperation of those with the capacity to prevent ongoing infringement").[10] In striking this balance, Congress was driven by the observation that unless copyright owners have the ability to protect their copyrights on the Internet, they will be less likely to make their works available online:

> Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy . . . [This legislation] will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of the American creative genius.

S. Rep. No. 105-190, at 8.

Congress also recognized that the Internet created unprecedented opportunities for copyright infringement, and sought to provide assistance to copyright owners in light of the technological developments surrounding the Internet:

> Copyright laws have struggled through the years to keep pace with emerging technology from the struggle over music played on a player

---

[10] "The DMCA affects [service providers'] liability by insulating [providers] from liability as long as they comply with certain statutory requirements designed to facilitate content providers' efforts to protect their copyrighted material." A. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 99 Geo. L.J. 1833, 1881 (2000).

> piano roll in the 1900's to the introduction of the VCR in the 1980's. With this constant evolution in technology, the law must adapt in order to make digital networks safe places to disseminate and exploit copyrighted materials . . . Title II [of the DMCA] clarifies the liability faced by service providers who transmit potentially infringing material over their networks. In short, Title II ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand.

S. Rep. No. 105-190, at 1-2. As Senator Leahy explained, "[t]he DMCA is a product of the Senate Judiciary Committee's recognition that ours is a time of unprecedented challenge to copyright protection . . . This bill is a well - balanced package of proposals that address the needs of creators, consumers and commerce in the digital age and well into the next century." *Id.* at 68.

Congress was concerned about the ability of copyright owners to protect their creative investments in light of rapid technological innovations on the Internet that make copyright theft easy, virtually instantaneous, and undetectable. Therefore, in exchange for the liability protections afforded to service providers in subsections (a) through (d) of the DMCA, Congress sought through subsection (h) to require service providers to assist copyright owners in identifying infringers using the service providers' systems. If, as Verizon contends, service providers only have such obligations when the infringing material is stored on their systems, then service providers falling within subsection (a) -- a large portion of those addressed by the DMCA -- would receive the liability protections of the Act without the corresponding obligation to assist copyright owners in identifying infringers. There is no logical

connection between the line Verizon seeks to draw and the objectives Congress sought to achieve through the DMCA. Verizon's reading would thus undermine the balance Congress established in the DMCA, and does not comport with the Act's purpose and history.[11] It is not for this Court to second-guess the compromises, negotiations, or even brokered deals that produced the DMCA; rather, the Court's role is to interpret the statute as enacted by Congress, and the clear language and structure of the DMCA must therefore control. *See Barnhart*, 534 U.S. at 460-61, 122 S. Ct. 941.

Complicating this assessment somewhat is the fact that two new technology developments underlying the issues in this case -- peer-to-peer (P2P) software and "bots," a software tool used by copyright owners to monitor the Internet and detect unauthorized distribution of copyrighted material -- were "not even a glimmer in anyone's eye when the DMCA was enacted" by Congress in 1998.[12] RIAA contends that P2P software makes Internet copyright piracy easy and immediate, while Verizon counters that "bots" will inundate service providers with thousands of computer-generated subpoenas seeking to identify infringers. Whether or not Congress was able to anticipate these technologies in enacting the DMCA, however, the courts cannot read new provisions or exceptions into a statute in order to accommodate future technological developments.

---

[11] This balance was adopted with substantial input from the service providers. In fact, the large service providers, including AOL and others, were heavily involved in negotiating these tradeoffs in the legislation. "Title II, for example, reflects 3 months of negotiations supervised by Chairman Hatch and assisted by Senator Ashcroft among the major copyright owners and the major OSP's and [Internet Service Providers]." S. Rep. No. 105-190, at 9.

[12] Br. of *Amicus Curiae* Alliance for Public Technology, *et al.*, at p. 6.

Particularly in the field of copyright, federal courts must defer to Congress' expertise and constitutional authority.

The Constitution assigns to Congress the authority to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. Const., art. I, § 8, cl. 8. The Supreme Court has long deferred to Congress on the scope and nuances of copyright law, especially regarding new technologies:

> Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably complicated by such new technology.

Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 431, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984); *see also Teleprompter Corp. v. CBS, Inc.*, 415 U.S. 394, 414, 94 S. Ct. 1129, 39 L. Ed. 2d 415 (1974) ("Detailed regulation of these relationships, and any ultimate resolution of the many sensitive and important problems in [the copyright] field, must be left to Congress."); *Fortnightly Corp. v. United Artists Television, Inc.*, 392 U.S. 390, 401, 88 S. Ct. 2084, 20 L. Ed. 2d 1176 (1968) (Court refused "to render a compromise decision . . . [to] accommodate various competing considerations of copyright, communications, and antitrust policy. We decline that invitation. That job is for Congress."). As recently as last week, the Supreme Court reiterated that "we defer substantially to Congress" on copyright law, that "we are not at liberty to second-guess congressional determinations and policy judgments" regarding copyright

issues, and that "it is generally for Congress, not the courts, to decide how best to pursue the Copyright Clause's objectives." *Eldred v. Ashcroft*, 537 U.S. 186, 123 S. Ct. 769, 772, 782, 785, 154 L. Ed. 2d 683 (2003) (citing *Sony Corp.*, 464 U.S. at 429, 104 S. Ct. 774, and *Stewart v. Abend*, 495 U.S. 207, 230, 110 S. Ct. 1750, 109 L. Ed. 2d 184 (1990)).

Notwithstanding these technological advancements, then, this Court will not attempt to re-balance the competing interests among service providers and copyright holders to address P2P software or "bots" that can roam the Internet detecting infringing material. As the Supreme Court stated in *Fortnightly*, "[t]hat job is for Congress." 392 U.S. at 401, 88 S. Ct. 2084. To date, Congress has spoken through the text, structure and purpose of the DMCA, under which, the Court concludes, RIAA's subpoena to Verizon meets the requirements spelled out in subsection (h) and therefore is valid.[13]

4. "John Doe" Actions As an Alternative

Verizon maintains that under its construction of the DMCA, with the subsection (h) subpoena power limited to service providers under subsection (c), owners would still have an adequate means to protect their copyrights. Verizon suggests that as an alternative RIAA may bring a "John Doe" action in federal court to obtain information identifying copyright infringers who, under subsection (a) of the DMCA, transmit infringing material over a service

---

[13] Verizon has not challenged RIAA's subpoena to Verizon on the ground that it does not meet the notification requirements under subsections (c)(3)(A) or (h)(2). RIAA provided a notification described in (c)(3)(A), including the identity of the copyright works infringed, a statement in good faith that the use of the works is not authorized, and a sworn declaration that the purpose of the subpoena is to obtain the identity of the infringer and that the information will only be used to protect rights to the copyright. *See* Motion to Enforce, Ex. B.

provider's network. As Verizon sees it, the copyright owner would file a complaint against John Doe, the unnamed infringer, and a third-party subpoena would then be issued and served on the service provider pursuant to Fed. R. Civ. P. 45. The service provider would then inform John Doe (its customer) of the lawsuit. Under this process, Verizon asserts, there would be protections, both procedural and substantive, for the user's rights, and service providers would have the opportunity to seek to quash the subpoena.

The short answer to Verizon's suggestion is that there is absolutely nothing in the DMCA or its history to indicate that Congress contemplated copyright owners utilizing John Doe actions in federal court to obtain the identity of apparent infringers, rather than employing the subsection (h) process specifically designed by Congress to address that need. Moreover, as Verizon concedes, the burden on service providers is certainly no greater with a DMCA subpoena than with a Rule 45 third-party subpoena.

The additional burden on copyright owners, however, would be considerable, given the effort and expense associated with pursuing such John Doe suits in court. Congress has noted the vast extent of copyright piracy over the Internet, and growing numbers of suits involving disputes over the sufficiency of allegations of infringement and other issues would, in turn, likely undermine the determination of copyright owners to prosecute such actions. Importantly, the time and delay associated with filing complaints and pursuing third-party subpoenas in court would undermine the ability of copyright owners to act quickly to prevent further infringement of their copyrights. That is at odds with the design of Congress through the DMCA, which commands "expeditious" issuance of and response to subpoenas under subsection (h). Moreover, Verizon overlooks altogether the burden on the

federal courts from large numbers of such actions. Federal courts have exclusive jurisdiction over copyright actions, and considering the extent of Internet copyright piracy could become inundated with John Doe actions seeking the identity of copyright infringers. *See NBC, Inc. v. Copyright Royalty Tribunal*, 848 F.2d 1289, 1295 (D.C. Cir. 1988) ("the federal courts . . . have exclusive jurisdiction over actions 'arising under' the Copyright Act, such as infringement actions"). Undoubtedly, the John Doe actions contemplated by Verizon would be more complex (involving three-party litigation) and time consuming than occasional enforcement actions for DMCA subpoenas.

Not only are John Doe actions more burdensome and less timely, but in several important ways they are less protective of the rights of service providers and Internet users than is the section 512(h) process. The DMCA mandates that a copyright holder fulfill several requirements under subsection (h) before the holder can obtain information from the service provider identifying the infringer. These protections ensure that a service provider will not be forced to disclose its customer's identifying information without a reasonable showing that there has been copyright infringement. Thus, to obtain a subsection (h) subpoena a copyright owner must have a "good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," § 512(c)(3)(A)(v), and must provide a "statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed," § 512(c)(3)(A)(vi). Moreover, Congress required a copyright owner to submit

> a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the

> identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

17 U.S.C. § 512(h)(2)(c). These requirements provide substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas. Indeed, they provide greater threshold protection against issuance of an unsupported subpoena than is available in the context of a John Doe action. And, of course, nothing in the DMCA precludes a service provider from raising non-compliance or other objections to a subsection (h) subpoena. *See, e.g., ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001) (action addressing service provider's resistance to subpoena for non-compliance with the DMCA).[14]

Given these various protections incorporated into the DMCA subpoena process,[15] the Court concludes that

---

[14] The DMCA also provides disincentives for false representations under the Act, making it costly for anyone to seek a subpoena on the basis of intentional misrepresentations, and thereby further ensuring that subpoenas will only be used in circumstances of good faith allegations of copyright infringement. Subsection (f) of the Act provides:

> Misrepresentations – Any person who knowingly materially misrepresents under this section (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer . . . or by a service provider, who is injured by such misrepresentations, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing . . ..

17 U.S.C. § 512(f).

[15] Indeed, the requirements for obtaining a section 512(h) subpoena are precisely the type of procedural requirements that other courts have imposed for subpoenas on service providers to identify anonymous posters of messages on the Internet. *See Doe v. 2TheMart.Com. Inc.*, 140 F.

Verizon's suggestion that John Doe actions are an adequate alternative remedy is not convincing. There is nothing in the DMCA to indicate that Congress intended that result. Such actions would be unworkable, far too slow, and uneconomical for copyright holders, and much too burdensome for the federal courts. Congress did not, in the Court's view, contemplate some service providers subject to the DMCA facing expeditious subsection (h) subpoenas, while others would only have to provide information identifying infringers through the slower, more cumbersome process of a John Doe action. Indeed, Verizon's suggestion would mean subpoenas under subsection (h) -- if limited to subsection (c) service providers -- would be delayed by complex factual issues involving whether a subsection (c) setting was actually presented, while subpoenas to all other service providers would be pursuant to even more burdensome, and slower, John Doe actions. Such a cumbersome, dual structure is flatly inconsistent with the "expeditious" subsection (h) subpoena process, and would run a serious risk of dissuading copyright owners from seeking the identity of apparent infringers and protecting their copyrights.[16] That result would be contrary to Congressional intent as evidenced in the text, structure and history of the DMCA.

Supp. 2d 1088, 1095 (W.D. Wash. 2001) (party seeking subpoena to service provider to identify anonymous non-party must show subpoena sought in "good faith" and that identifying information sought is directly and materially relevant to core claim and unavailable from any other source); *see also Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 578-79 (N.D. Cal. 1999).

[16] When the Court asked Verizon's counsel whether John Doe actions might be so expensive that they would "scare off" copyright owners, he responded that "[t]here is that possibility" given the protections and "hoops that have to be gone through under the John Doe suits." Tr. of Hearing (Oct. 4, 2002) at p. 62.

5. The DMCA and the Constitution

A number of possible constitutional challenges to the subsection (h) subpoena power have been identified by *amici curiae*. Verizon, however, does not assert that the subpoena power in subsection (h), as applied to service providers (like Verizon) under subsection (a), is unconstitutional; instead, Verizon merely states that it "raises substantial questions."[17] RIAA accordingly has not fully briefed the various constitutional issues raised by the *amici curiae* supporting Verizon. Hence, the Court is without the benefit of full development of these issues by the parties.

Unless raised by the parties, a court normally should not entertain statutory or constitutional challenges asserted solely by *amici*. *See, e.g., A.D. Bedell Wholesale Co. v. Philip Morris Inc.*, 263 F.3d 239, 266 (3d Cir. 2001) ("Although the Cato Institute, *amicus curiae* for plaintiffs, argues constitutional claims, new issues raised by an *amicus* are not properly before the court in the absence of exceptional circumstances.") (quoting *General Eng'g Corp. v. Virgin Islands Water and Power Auth.*, 805 F.2d 88, 92 (3d Cir. 1986)). Indeed, in construing the DMCA, the Second Circuit refused to consider a constitutional challenge briefly addressed by the defendant in a footnote, although fully examined by an *amicus*. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001). Without a "properly developed record," the court found that the defendant effectively waived the constitutional challenge: "Although an *amicus* brief can be helpful in elaborating issues properly presented by the parties, it is normally not a method for injecting new issues

---

[17] Verizon devotes only two sentences and a footnote to the constitutional issues, contending that the subsection (h) subpoena authority, if broadly construed, raises substantial Article III (judicial power) and First Amendment (freedom to engage in anonymous speech) questions. *See* Verizon Opp. at p. 4.

..., at least in cases where the parties are competently represented by counsel." *Id.* at 445. Here, because Verizon is not raising any explicit constitutional challenge to the DMCA, the Court is wary of considering such issues.[18]

Even if the Court were to consider a constitutional challenge here, it must be noted that any constitutional problems faced by service providers or their customers would exist under Verizon's construction of the DMCA as well. The Court's authority and users' anonymity are equally at issue with subsection (c) as with subsection (a), and the First Amendment interest -- the identity of the user -- is identical no matter which subsection is invoked.

It is also clear that the First Amendment does not protect copyright infringement. *See Harper & Row, Publs., Inc. v. Nation Enters.*, 471 U.S. 539, 555-60, 105 S. Ct. 2218, 85 L. Ed. 2d 588 (1985); *Zacchini v. Scripps- Howard*, 433 U.S. 562, 574-78, 97 S. Ct. 2849, 53 L. Ed. 2d 965 (1977). Moreover, the Supreme Court recently confirmed in *Eldred v. Ashcroft* that the proximity of the Copyright Clause and the First Amendment demonstrates "the Framers' view [that] copyright's limited monopolies are compatible with free speech principles," and that copyright serves to promote First Amendment ideals as "'the engine of free expression.'" 123 S. Ct. at 788 (quoting *Harper & Row*, 471 U.S. at 558, 105 S. Ct. 2218). The Court noted "built-in First Amendment accommodations" in copyright law, including the distinction between ideas and expression and the "fair use" doctrine, which it found "are generally adequate to address" First Amendment concerns relating to asserted rights to use the speech of others. *Id.* at 788-89; *see Nihon Keizai Shimbun, Inc.*

---

[18] RIAA and Verizon have acknowledged that Verizon may not have standing to raise a challenge to the subpoena based on the user's alleged First Amendment or other constitutional interests. The Court need not address that issue here.

v. Comline Bus. Data, Inc., 166 F.3d 65, 74 (2d Cir. 1999) ("We have repeatedly rejected First Amendment challenges to injunctions from copyright infringement on the ground that First Amendment concerns are protected by and coextensive with the fair use doctrine."). Here, of course, the various protections incorporated into subsection (h), and discussed *supra*, further guard against First Amendment concerns.

Nor is this an instance where the anonymity of an Internet user merits free speech and privacy protections. Certainly, the Supreme Court has recognized that, in some situations, the First Amendment protects a speaker's anonymity. *See, e.g., Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 122 S. Ct. 2080, 2090, 153 L. Ed. 2d 205 (2002) (municipal ordinance requiring pamphleteers to disclose names implicates "anonymity interests" rooted in the First Amendment); *Buckley v. Am. Constitutional Law Foun., Inc.*, 525 U.S. 182, 119 S. Ct. 636, 142 L. Ed. 2d 599 (1999) (state requirement forcing petitioners to wear identification badge violated First Amendment because it infringed on petitioners' anonymity); *McIntyre v. Ohio Elections Comm.*, 514 U.S. 334, 115 S. Ct. 1511, 131 L. Ed. 2d 426 (1995) (the right to speak anonymously "exemplifies the purpose behind the Bill of Rights, and the First Amendment in particular"). Lower federal courts have specifically recognized that the First Amendment may protect an individual's anonymity on the Internet. *See, e.g., Doe v. 2TheMart.Com, Inc.*, 140 F. Supp. 2d at 1097 ("the constitutional rights of Internet users, including the right to speak anonymously, must be carefully safeguarded"); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998), *aff'd*, 194 F.3d 1149 (10th Cir. 1999) (upholding First Amendment right to communicate anonymously over the Internet); *ACLU of Georgia v. Miller*, 977 F. Supp. 1228, 1230 (N.D. Ga. 1997) (recognizing constitutional right to communicate anonymously and

pseudonymously on the Internet). The Internet and Worldwide Web provide an unprecedented electronic megaphone for the expression of ideas and an unparalleled opportunity for a national--even international--town square for expression. *See, e.g., Reno v. ACLU*, 521 U.S. 844, 853, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997) ("Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox.").

But neither Verizon nor any *amici* has suggested that anonymously offering for downloading more than 600 songs over the Internet without authorization is protected expression under the First Amendment.[19] To be sure, this is not a case where Verizon's customer is anonymously using the Internet to distribute speeches of Lenin, Biblical passages, educational materials, or criticisms of the government--situations in which assertions of First Amendment rights more plausibly could be made. As the Supreme Court explained in *Watchtower Bible & Tract Society*, the purpose of protecting anonymous expression is to safeguard those "who support causes anonymously" and those who "fear economic or official retaliation," "social ostracism," or an unwanted intrusion into "privacy." 122 S. Ct. at 2089. The materials RIAA alleges are being infringed include more than 600 copyrighted recordings by well-known artists. RIAA has shown that the copyright owners have not authorized such use; moreover, the fact that these copyrighted materials were shared over the peer-to-peer software of KaZaA only reinforces the belief that copyrights are being infringed. There is no evidence, or even suggestion, in the record to indicate that downloading or

---

[19] RIAA notes, moreover, that the alleged infringer is not truly anonymous--Verizon knows the identity.

transmitting these recordings is somehow protected expression.[20]

Interestingly, Verizon's argument that a copyright owner seeking to obtain information about an alleged infringer should use a John Doe action undercuts the contention that the DMCA subpoena process violates the Internet user's right to anonymity. The First Amendment problems, if any, would be the same in either litigation setting, and the user could assert its rights and objections to either subpoena.[21] Hence, if the John Doe action alternative poses no First

---

[20] The Ninth Circuit has twice upheld injunctions ordering a defendant to disable its file transferring service and shut down the service, without finding any First Amendment violation. *See A & M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002); *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001) ("First Amendment concerns in copyright are allayed by the presence of the fair use doctrine" and "[u]ses of copyrighted material that are not fair uses are rightfully enjoined"). This Court, however, is not being asked to enjoin the peer-to-peer software used here; litigation against KaZaA is proceeding in other courts across the country. All that is at issue here is the identity of the apparent infringer using Verizon's system, and whether the DMCA requires Verizon to produce that limited information.

[21] The *amici* also challenge the subsection (h) subpoena power on the ground that under Article III of the Constitution there must be a "case or controversy" before the Court to provide jurisdiction to issue a subpoena. Again, Verizon has made it clear that it is not raising an Article III challenge to the DMCA, but only noting a "policy consideration" relevant in interpreting the DMCA, and there has been no briefing on this issue by the parties. *See* Tr. of Hearing (Oct. 4, 2002) at p. 61. Of course, the DMCA includes a provision in subsection (h)(6) requiring that the issuance and enforcement of subpoenas "shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum." That protection ensures that service providers served with subpoenas can resort to the Federal Rules, including Fed. R. Civ. P. 45, which specifically addresses subpoena enforcement and the rules for quashing a subpoena.

Amendment issue, the subsection (h) subpoena process does not either.

The Court does not, however, resolve the constitutional issues identified by Verizon and several *amici*. Absent a clear challenge by Verizon, and full briefing and development by the parties, it is not appropriate to do so. But certainly the issues raised do not reveal an obviously fatal constitutional flaw in the subpoena process available under the DMCA.[22]

CONCLUSION

Based on the text and structure of the Digital Millennium Copyright Act, as confirmed by the purpose and history of the Act, the Court concludes that the subpoena authority of section 512(h) applies to all service providers within the coverage of the Act, including Verizon and other service providers falling within subsection (a). With copyright legislation such as the DMCA, "[t]he wisdom of Congress' action . . . is not within [the Court's] province to second guess." *Eldred v. Ashcroft*, at 790. Therefore, the Court grants RIAA's motion to enforce its subpoena, and orders Verizon to comply with the subpoena. A separate order has been issued on this date.

---

[22] Arguably, a First Amendment challenge by Verizon would be facial rather than as applied, and thus it would have to be shown that in virtually every application the DMCA offends the First Amendment by requiring the production of the identity of an anonymous user. *See United States v. Salerno*, 481 U.S. 739, 745, 107 S. Ct. 2095, 95 L. Ed. 2d 697 (1987). That is a heavy burden for Verizon to satisfy.

Appendix C

United States District Court,
District of Columbia.

In re: VERIZON INTERNET SERVICES, INC.,
Subpoena Enforcement Matter,
Recording Industry Association of America, Plaintiff,
v.
Verizon Internet Services, Defendant.

No. CIV.A. 03-MS-0040 JDB.

April 24, 2003.

MEMORANDUM OPINION

BATES, District Judge.

Before the Court is the motion of Verizon Internet Services ("Verizon") to quash the February 4, 2003 subpoena served on it by the Recording Industry Association of America ("RIAA") pursuant to the Digital Millennium Copyright Act of 1998 ("DMCA"), 17 U.S.C. § 512. On behalf of copyright owners, RIAA seeks the identity of an anonymous user of the conduit functions of Verizon's Internet service who is alleged to have infringed copyrights by offering hundreds of songs for downloading over the Internet.[1] In an earlier action, this Court rejected Verizon's statutory challenges to a similar subpoena, holding that Verizon's conduit functions were within the scope of the subpoena authority of § 512(h) of the DMCA. *See In re:*

---

[1] RIAA is the industry trade association for sound and music recordings, and is authorized to enforce the copyrights of its members, who create and distribute most of the music sold in the United States.

Verizon Internet Services, Inc., Subpeona Enforcement Matter, 240 F. Supp. 2d 24 (D.D.C. 2003). Verizon now claims that § 512(h) violates Article III of the Constitution because it authorizes federal courts to issue binding process in the absence of a pending case or controversy, and that § 512(h) violates the First Amendment rights of Internet users. If the merits of Verizon's constitutional challenges are rejected by this Court, Verizon seeks a stay pending appeal of that ruling, and of the earlier statutory ruling by this Court.

Having considered the parties' several memoranda, three hearings, the brief of the United States as intervenor defending the constitutionality of § 512(h), a number of *amicus* briefs, and the entire record herein, the Court denies Verizon's motion to quash RIAA's February 4, 2003 subpoena. The subpoena power authorized under § 512(h) of the DMCA does not violate the case or controversy requirement of Article III and does not abridge the First Amendment rights of Internet users. Moreover, because Verizon is unable to show irreparable harm or that it is likely to succeed on an appeal of its constitutional or statutory challenges, the Court also denies Verizon's request for a stay pending appeal.[2]

I. PROCEDURAL HISTORY

This case has followed a somewhat circuitous procedural path. To begin with, this is the second subpoena RIAA has served on Verizon pursuant to the DMCA seeking the identity of an anonymous Internet user alleged to have infringed protected copyrights. On July 24, 2002, RIAA served its first subpoena to obtain the identity of a Verizon subscriber alleged to have made more than 600 copyrighted songs available for downloading over the Internet through

---

[2] A temporary stay of 14 days will be entered to enable Verizon to seek a stay in the Court of Appeals.

peer-to- peer file transfer software provided by KaZaA. Verizon claimed that because RIAA's subpoena related to material transmitted over Verizon's network -- rather than stored on it -- it fell outside the scope of the subpoena power authorized by § 512(h). Verizon read § 512(h) as applying only in those situations where the infringing material is physically stored on the service provider's network. RIAA contended that the subpoena authority under § 512(h) applied to all service providers under the DMCA, including Verizon. The parties framed the issue as one of statutory construction, although Verizon noted that if § 512(h)'s subpoena authority were construed as applying to all service providers, the statute "raises substantial questions" under Article III and the First Amendment.

The Court construed the subpoena power in § 512(h) as applying to all service providers under the DMCA, and granted RIAA's motion to enforce the subpoena. *See In re: Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24 (hereinafter "*First Subpoena Decision*"). The Court did not reach the constitutional arguments, instead deciding the question strictly on statutory grounds by construing the DMCA's language, structure, purpose, and legislative history. As a result, the Court found the subpoena valid and ordered Verizon expeditiously to provide RIAA with the identity of the subscriber alleged to be infringing copyrighted songs.

Verizon appealed that decision, and moved to stay the Court's order pending resolution of its appeal.[3] In its motion for a stay, Verizon asserted constitutional challenges as the primary basis for a stay, claiming that the Court's construction of § 512(h) raised serious questions regarding the First Amendment rights of Internet users and presented

---

[3] Pursuant to Fed. R. App. P. 8(a), this Court ordered a temporary stay to allow the issues to be fully briefed and decided.

a critical issue whether a subpoena could issue under Article III without an actual "case or controversy" pending in federal court. RIAA contended that because Verizon had not raised these issues earlier, it had waived them on appeal.

The Court held a hearing on Verizon's stay motion. Meanwhile, however, RIAA served a *second* subpoena on Verizon on February 4, 2003. Shortly after the hearing on its motion to stay the first subpoena, Verizon moved to quash RIAA's second subpoena, directly presenting the constitutional challenges.[4] In an effort to resolve both the motion to stay on the first subpoena and the constitutional challenges to the second subpoena, the Court ordered another round of expedited briefing. Verizon proposed notifying the two subscribers whose conduct is at issue of the commencement and status of these actions, and the nature of RIAA's allegations of copyright infringement, which was then done at the Court's urging. A third hearing to address Verizon's constitutional challenges to § 512(h) was held on April 1, 2003. Subsequently, the United States has moved, and been permitted, to intervene and has submitted a brief defending the constitutionality of the DMCA.

The gravamen of Verizon's statutory challenge to the first subpoena was that the subpoena power under § 512(h) should be construed as limited to situations within § 512(c) where allegedly infringing material is stored on the Internet service provider's network. This Court firmly rejected that view in *First Subpoena Decision*, 240 F. Supp. 2d 24. The constitutional challenges now asserted by Verizon in response to the second RIAA subpoena are, although

---

[4] Because the second subpoena involved the same parties as the first subpoena and related legal issues, Verizon's motion to quash was assigned to this judge with the agreement of both Verizon and RIAA.

substantive and in apparent good faith, somewhat in tension with the earlier statutory challenge. If Verizon were correct that § 512(h) should be construed to permit subpoenas only for subsection (c) service providers -- which it is not -- Verizon's Article III challenge would nonetheless retain its full force because such subpoenas would still, under Verizon's view, be unconnected to a pending case or controversy, and the asserted First Amendment concerns would also remain, albeit focused on the more limited subset of subscribers of subsection (c) service providers. Given this tension, one might ask why the constitutional challenges were not more fully pressed by Verizon in the first subpoena litigation. Be that as it may, those issues are now squarely before the Court in this case.[5]

II. SECTION 512(h) DOES NOT VIOLATE ARTICLE III

Verizon contends that § 512(h) violates Article III of the Constitution because it authorizes federal courts to issue subpoenas in the absence of a pending case or controversy. Citing cases from the eighteenth and nineteenth centuries, Verizon argues that federal judges can neither exercise authority outside the context of an actual case or controversy nor undertake non-judicial functions. *See Hayburn's Case*, 2 U.S. (2 Dall.) 408, 1 L. Ed. 436 (1792); *United States v. Ferreira*, 54 U.S. 40, 13 How. 40, 14 L. Ed. 40 (1851). Relying on *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 108 S. Ct. 2268, 101 L. Ed. 2d 69 (1988), and *Houston Business Journal, Inc. v. Office of the Comptroller of the Currency*, 86 F.3d 1208 (D.C. Cir. 1996), Verizon also argues more specifically that "the power to issue subpoenas exists only in the context of a case that is properly pending before

---

[5] Because the *First Subpoena Decision* provided an extensive overview of § 512 of the DMCA, the Court will not repeat that explanation here, and instead incorporates that background discussion by reference.

a federal court." Verizon's Br. Supp. Mot. Quash Feb. 4, 2003 Subpoena at 12.[6]

Verizon's arguments, although intriguing, are ultimately not persuasive. No doubt the justices of the Supreme Court have indicated that the federal courts are properly confined to the exercise of "judicial power." *See Hayburn's Case*, 2 U.S. at 410 n.*, 2 Dall. 409; *Ferreira*, 54 U.S. at 48, 13 How. 40.[7] And, more recently, the Supreme Court has noted that "[f]ederal judicial power itself extends only to adjudication of cases and controversies and it is natural that its investigative powers should be jealously confined to these ends." *United States v. Morton Salt Co.*, 338 U.S. 632, 641-642, 70 S. Ct. 357, 94 L. Ed. 401 (1950). But upon examination, it is clear that the § 512(h) subpoena authorization does not represent an innovation that is inconsistent with the limited role of the judiciary as it has traditionally been understood in our constitutional regime.

---

[6] To be clear, Verizon does not contend that the instant proceeding to quash a subpoena is not a case or controversy; rather, Verizon contends that the issuance of the subpoena under § 512(h) does not constitute, and was not conducted in the context of, a case or controversy. It is well-established that courts may hear an action to enforce or quash a subpoena even where the subpoena was not issued in connection with a case pending in the federal courts. *See ICC v. Brimson*, 154 U.S. 447, 490, 14 S. Ct. 1125, 38 L. Ed. 1047 (1894) (courts may aid inquiries before the ICC); *United States v. Hill*, 694 F.2d 258, 269 (D.C. Cir. 1982) (court has jurisdiction to enforce investigatory subpoenas issued by the Department of Energy).

[7] The Supreme Court itself did not reach the constitutional issue in *Hayburn's Case*, but the opinions of several Circuit Courts (on which certain Justices of the Supreme Court sat) "were reported in the margins of the Court's decision in that case, and have since been taken to reflect a proper understanding of the role of the Judiciary under the Constitution." *Morrison v. Olson*, 487 U.S. 654, 678 n. 15, 108 S. Ct. 2597, 101 L. Ed. 2d 569 (1988).

As an initial matter, the clerk's issuance of a § 512(h) subpoena does not involve either the exercise of judicial power or the exercise by federal judges of Article I or Article II-type investigatory power. Indeed, the issuance of a § 512(h) subpoena cannot properly be considered an act of "the court." Subsection (h)(4) provides that "[i]f the notification [of claimed infringement] filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk **shall** expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider." 17 U.S.C. § 512(h)(4) (emphasis added). Under this subsection, the clerk exercises no discretion; if the requirements are met, the subpoena must be issued. The clerk, in other words, executes a quintessentially ministerial duty. *See Mississippi v. Johnson*, 71 U.S. (4 Wall.) 475, 498, 18 L. Ed. 437 (1866) ("A ministerial duty ... is one in respect to which nothing is left to discretion. It is a simple, definite duty, arising under conditions admitted or proved to exist, and imposed by law."); *Nealon v. Davis*, 18 F.2d 175, 176 (D.C. Cir. 1927) ("A ministerial act is one which a person performs in a given state of facts, in a prescribed manner, in obedience to the mandate of legal authority, without regard to, or the exercise of his own judgment upon the propriety of the act being done." (citation and internal quotation marks omitted)). In fact, the legislative history of § 512(h) indicates that Congress specifically intended the issuance of the subpoena to "be a ministerial function." S. Rep. No. 105-190, at 51 (1998).

Stretching back to the days of Chief Justice Marshall, the Supreme Court has repeatedly distinguished between actions that are ministerial in nature and those that constitute an exercise of judicial, legislative, or discretionary executive power. *See, e.g., Custiss v. Georgetown & Alexandria*

Turnpike Co., 6 Cranch 233, 10 U.S. 233, 237, 3 L. Ed. 209 (1810) (Marshall, C.J.) (clerk's act of recording an inquisition signed by marshal and jurymen is a "ministerial act which the law directs the clerk to perform ... and requires no exercise of judicial functions"); *Elliot v. Lessee of William Peirsol*, 26 U.S. 328, 341, 1 Pet. 328, 7 L. Ed. 164 (1828) (in making and recording a certificate of acknowledgment of a deed, clerk of court "acted ministerially, and not judicially"); *Ex parte Virginia*, 100 U.S. 339, 348, 10 Otto 339, 25 L. Ed. 676 (1879) (selection of jurors "surely is not a judicial act" but "is merely a ministerial act"); *Central Loan & Trust Co. v. Campbell Comm'n Co.*, 173 U.S. 84, 95, 19 S. Ct. 346, 43 L. Ed. 623 (1899) (probate judge's grant of an order for attachment did "not involve the discharge of a judicial function but merely the performance of a ministerial duty"); *ICC v. Chicago Great W. Ry. Co.*, 209 U.S. 108, 117-18, 28 S. Ct. 493, 52 L. Ed. 705 (1908) (positing distinction between duties that are "ministerial, and therefore such as may legally be imposed upon a ministerial body" and those that are "legislative, and therefore, under the Federal Constitution, a matter for congressional action"); *Wells v. Roper*, 246 U.S. 335, 338, 38 S. Ct. 317, 62 L. Ed. 755 (1918) (decision by Postmaster General and his deputy to cancel contract "was executive in character, not ministerial, and required an exercise of official discretion"); *District of Columbia Court of Appeals v. Feldman*, 460 U.S. 462, 479, 103 S. Ct. 1303, 75 L. Ed. 2d 206 (1983) (District of Columbia Court of Appeals acted judicially, not ministerially, in considering petitions for waiver of bar admission requirements).[8] Chief Justice Marshall specifically noted in *Custiss* that "the legislature

---

[8] *See also Dornan v. Sanchez*, 978 F. Supp. 1315, 1326 (C.D. Cal. 1997) (court's issuance of subpoenas in connection with election contest to be adjudicated by House of Representatives is a "ministerial" function that does not require the court to "exercise its own judicial power").

may direct the clerk of a court to perform a specified service, without making his act the act of the court." 10 U.S. at 236, 6 Cranch 233.

Here, the fact that Congress has directed an employee of the judicial branch to carry out a specific non-discretionary function neither implicates Article III judicial power nor involves federal judges in an investigation of the sort properly relegated to one of the other branches. In a real-world sense, no Article III judge takes any action with respect to a § 512(h) subpoena until the copyright holder moves to enforce the subpoena or the service provider moves to quash it--at which time there is a concrete controversy sufficient to confer jurisdiction under Article III of the Constitution.

Verizon objects to this line of analysis, arguing that a § 512(h) subpoena is issued in the name of the district court and thus should be treated as an act of the court. And, indeed, it is true that because the procedures in Fed.R.Civ.P. 45 governing enforcement of a subpoena *duces tecum* are applicable to a § 512(h) subpoena, *see* 17 U.S.C. § 512(h)(6), a service provider's failure to comply with a § 512(h) subpoena could, like a failure to comply with a Rule 45 subpoena, be construed as a violation of a court order, providing a basis for contempt sanctions. *See Waste Conversion, Inc. v. Rollins Envtl. Servs. (NJ). Inc.*, 893 F.2d 605, 608 (3d Cir. 1990) (en banc) (assuming "for purposes of this appeal," that failure to comply with a Rule 45 subpoena for testimony could subject a person to criminal contempt); *Fisher v. Marubeni Cotton Corp.*, 526 F.2d 1338, 1340 (8th Cir. 1975) ("A subpoena is a lawfully issued mandate of the court issued by the clerk thereof."); Fed. R. Civ. P. 45 advisory committee notes for 1991 amendment ("Although the subpoena is in a sense the command of the attorney who completes the form, defiance of a subpoena is nevertheless

an act in defiance of a court order and exposes the defiant witness to contempt sanctions."). But even in the Rule 45 context, courts recognize that a subpoena issued upon express order of a judge and a subpoena issued by the clerk of the court are not equivalent. *See Waste Conversion*, 893 F.2d at 608 ("A subpoena, obtainable as of course from the Clerk of the Court, is not of the same order as one issued by a judicial officer in the resolution of a specific dispute."); *Daval Steel Prods. v. M/V Fakredine*, 951 F.2d 1357, 1364 (2d Cir. 1991) (same); Fed. R. Civ. P. 45 advisory committee notes for 1991 amendment ("But, because the command of the subpoena is not in fact one uttered by a judicial officer, contempt should be very sparingly applied when the nonparty witness has been overborne by a party or attorney."); *see also Doe v. DiGenova*, 779 F.2d 74, 85 (D.C. Cir. 1985) (grand jury subpoena is not an "order of a court" unless specifically approved by a court). The better view here is that because the issuance of a § 512(h) subpoena is a ministerial task accomplished without judicial involvement, it does not implicate Article III judicial power or improperly place federal judges in an investigatory role.

In any event, assuming that the issuance of a § 512(h) subpoena can be conceptualized as a judicial act, Verizon's challenge still fails. In the first place, § 512(h) is by no means as unique as Verizon claims. Congress has enacted several provisions that specifically authorize the clerk of the district court to issue subpoenas despite the absence of a pending case or controversy in the federal courts. *See, e.g.*, 2 U.S.C. § 388 (subpoenas for depositions in connection with proceedings in the House of Representatives); 35 U.S.C. § 24 (subpoenas for evidence to be used in connection with proceedings in Patent and Trademark Office); 45 U.S.C. § 157(h) (subpoenas at the request of arbitrators under the Railway Labor Act); 7 U.S.C. § 2354(a) (subpoenas for evidence to be used in connection with proceedings in Plant

Variety Protection Office). Moreover, these provisions are not recent innovations but rather were firmly established by the time that § 512(h) was enacted in 1998. *See Dornan*, 978 F. Supp. at 1319 (noting that precursor to 2 U.S.C. § 388 was enacted in 1798); Act of July 8, 1870, ch. 230, § 44, 16 Stat. 204 (original source of 35 U.S.C. § 24); Railway Labor Act, ch. 347, § 7, 44 Stat. 577 (1926) (original source of 45 U.S.C. § 157(h)); Pub.L. 91-577, tit. I, § 24, 84 Stat. 1544 (1970) (original source of 7 U.S.C. § 2354(a)).

But even setting aside these particular provisions, it is clear that "federal courts and judges have long performed a variety of functions that . . . do not necessarily or directly involve adversarial proceedings within a trial or appellate court." *Morrison*, 487 U.S. at 681 n. 20, 108 S. Ct. 2597; *see also United States v. Reagan*, 453 F.2d 165, 173 n.4 (6th Cir. 1971) ("The invocation of judicial power prior to formal charges being made or before filing suit is indeed a common practice in our jurisprudence."). In the criminal context, for example, courts issue warrants, *see* Fed. R. Crim. P. 41, and review applications for wire taps, *see* 18 U.S.C. §§ 2516, 2518, "both of which may require a court to consider the nature and scope of criminal investigations on the basis of evidence submitted in an *ex parte* proceeding." *Morrison*, 487 U.S. at 681 n.20, 108 S. Ct. 2597. Courts also assist grand juries in their investigative function by compelling the testimony of witnesses, despite the absence of a traditional adversarial proceeding. *See id.*[9] And Congress has authorized district

---

[9] Verizon baldly asserts that the § 512(h) subpoena context cannot "be analogized to the textually assigned judicial roles of checking Executive power in grand jury investigations and applications for search warrants." *See* Verizon's Reply Br. Supp. Mot. Quash at 2 n.3 (citing U.S. Const. amends. IV & V). But the proposition that in these settings courts serve to check Executive power does not undermine the overarching fact that the Constitution acknowledges roles for the judiciary outside the context of a classic case or controversy.

courts to require testimony or other evidence for use in a foreign tribunal, even where no proceeding is yet pending in that forum. *See* 28 U.S.C. § 1782(a); *In re: Letter Rogatory*, 42 F.3d 308, 310 (5th Cir. 1995) ("Congress abrogated the requirement that the foreign litigation actually be pending before relief could be had under § 1782.").[10]

In the civil context, perhaps the most deeply rooted analogue to § 512(h) is Fed. R. Civ. P. 27(a). That provision reflects the traditional powers of the courts at equity dating from even before the adoption of the Constitution, *see Arizona v. California*, 292 U.S. 341, 347, 54 S. Ct. 735, 78 L. Ed. 1298 (1934), and allows a federal court to authorize a person to perpetuate testimony by deposition before an action is filed where doing so would "prevent a failure or delay of justice." Fed. R. Civ. P. 27(a)(3). In order to obtain a Rule 27(a) order, the petitioner seeking testimony must show

> 1, that the petitioner expects to be a party to an action cognizable in a court of the United States but is presently unable to bring it or cause it to be brought, 2, the subject matter of the expected action and the petitioner's interest therein, 3, the facts which the petitioner desires to establish by the proposed testimony and the reasons for desiring to perpetuate it, 4, the names or a description of the persons the petitioner expects will be adverse parties and their addresses so far as known, and 5, the names and addresses of the persons to be examined and the substance of the testimony which the petitioner expects to elicit from each.

---

[10] Moreover, as the United States points out, in the § 1782 setting it is unlikely there will ever be an underlying claim within federal court jurisdiction because the proceeding in the foreign tribunal arises under foreign, not American, law. *See* Br. Intervenor United States at 8.

Fed. R. Civ. P. 27(a)(1).

Notably, the requirements for obtaining a § 512(h) subpoena are similarly rigorous. A copyright owner (or a person authorized to act on the owner's behalf) must present to the clerk a proposed subpoena, "a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under [Title 17]," and a copy of the notification of claimed infringement. 17 U.S.C. § 512(h)(1), (2). This notification, in turn, must include "substantially the following":

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Id. § 512(c)(3). Thus, under both Rule 27(a) and § 512(h), private parties may avail themselves of judicial machinery to obtain information prior to the filing of a complaint -- but only if they satisfy a specific set of criteria and identify with particularity the information they seek to compel.

For its part, Verizon argues vigorously that Rule 27(a) is not sufficiently analogous to § 512(h) to be instructive. Primarily, Verizon contends that Rule 27(a) is distinguished by its requirement for a clear allegation of intent to file a lawsuit. *See* 8 Charles A. Wright, Arthur R. Miller, & Richard L. Marcus, Federal Practice and Procedure § 2072 (2d ed. 1994). Under § 512(h), Verizon points out, the subpoena application need not even come from the copyright holder -- the real party-in-interest with standing to bring a lawsuit. In addition, Verizon argues, Rule 27(a) does not allow actual discovery but only the preservation of evidence where necessary, *see Penn Mut. Life Ins. Co. v. United States*, 68 F.3d 1371, 1376 (D.C. Cir. 1995), and allows the adverse party the opportunity to contest the petition to perpetuate testimony, *see* Fed. R. Civ. P. 27(a)(2).

These differences, however, are neither as substantial nor as consequential as Verizon contends. First, although an entity seeking a subpoena under § 512(h) need not state that it expects to be a party to an action cognizable in federal

court, it does have to make a sworn statement of good faith belief that a copyright is being used in an unauthorized manner--a statement largely to the effect that a copyright action cognizable in federal court could be asserted (if not by the party seeking the subpoena then by its principal, the copyright holder). Thus, § 512(h), like Rule 27(a), requires as a prerequisite to court action a significant showing as to the existence of a breach or violation into which the court could ultimately be drawn. Moreover, in neither the Rule 27(a) nor the § 512(h) setting can the court be certain that a judicial action will ever be filed. *See Penn Mut.*, 68 F.3d at 1374 ("[A] party need not demonstrate that litigation is an absolute certainty in order to perpetuate testimony pursuant to Rule 27(a).").

With respect to Verizon's distinction between discovery and preservation of evidence under Rule 27(a), it is undisputed that some service providers (although not Verizon) might log only temporarily the identifying information sought on a § 512(h) subpoena. *See* Tr. of April 1, 2003, Hearing at 14-15; Declaration of Frank Creighton ¶ 16. Hence, § 512(h), like Rule 27(a), provides a method for preserving, not merely discovering, information essential to a potential lawsuit. Also lacking in merit is Verizon's argument that Rule 27(a) is distinguished by the possibility of adversarial proceedings contesting the petition. The alleged infringer may receive no notice of a § 512(h) subpoena before his identity is released, but the entity subpoenaed (the service provider) does have the opportunity to contest the subpoena in federal court before it is enforced. *See, e.g., ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001) (action addressing service provider's resistance to DMCA subpoena). In other words, § 512(h) does not authorize an entirely *ex parte* form of judicial compulsion.

Overall then, despite Verizon's objections, Rule 27(a) provides a compelling precedent for judicial compulsion of information outside the context of a pending case or controversy. Furthermore, taking Rule 27(a) together with the other analogues discussed above, there is ample basis for the Court to conclude that the role assigned to the clerk of the court in § 512(h) is countenanced by the Constitution.

Notwithstanding Verizon's contentions, *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 108 S. Ct. 2268, 101 L. Ed. 2d 69 (1988), and *Houston Business Journal, Inc. v. Office of the Comptroller of the Currency*, 86 F.3d 1208 (D.C. Cir. 1996), do not undermine this conclusion. In *Catholic Conference*, the Supreme Court held that where a district court lacks subject matter jurisdiction over an action, it also lacks power to issue a contempt citation for failure to comply with a subpoena issued in connection with that action. 487 U.S. at 80, 108 S. Ct. 2268. In *Houston Business Journal*, the D.C. Circuit held that a district court lacks power to issue a subpoena when the underlying action is asserted in state, not federal, court. 86 F.3d at 1213.

Importantly, in both *Catholic Conference* and *Houston Business Journal*, the only conceivable source for the district court's jurisdiction to issue a subpoena was a pending case or controversy; it was the absence of a sound federal case or controversy that was thus fatal to the validity of the subpoenas in question. Here, in contrast, Congress has expressly provided the clerk of the court with the authority to issue § 512(h) subpoenas; thus the clerk need not draw upon the powers arising from jurisdiction over a pending case or controversy. Section 512(h) accordingly presents a situation neither expressly contemplated nor ruled out by the holdings in *Catholic Conference* and *Houston Business Journal*. Indeed, the D.C. Circuit implicitly recognized in

Houston Business Journal that in settings such as Rule 27(a) the federal courts' subpoena power may properly be asserted in the absence of subject matter jurisdiction over an underlying action. *See* 86 F.3d at 1213.

Verizon seeks to bolster its position by arguing that § 512(h) offends the policy concerns that underlie the case-or-controversy requirement. According to Verizon, this requirement "ensures both that the judiciary does not take on non-adjudicatory tasks and that neither Congress nor the Executive attempts to foist non-judicial duties on the Article III courts." Verizon's Br. Supp. Mot. Quash at 5 (emphasis omitted). Duties that are inconsistent with the judicial function, Verizon contends, "undermine public confidence in the independence and impartiality of the judiciary and take the courts' resources away from their primary role." *Id.* By putting the judiciary in the role of the copyright holder's "investigator," Verizon maintains, § 512(h) implicates both of these concerns.

The Court does not agree. In *Morrison v. Olson*, the Supreme Court identified two principal concerns underlying the general rule, derived from the case-or-controversy requirement, that "'executive or administrative duties of a nonjudicial nature may not be imposed on judges holding office under Art. III of the Constitution.'" 487 U.S. at 677, 108 S. Ct. 2597 (quoting *Buckley v. Valeo*, 424 U.S. 1, 123, 96 S. Ct. 612, 46 L. Ed. 2d 659 (1976)). First, the rule "help[s] ensure the independence of the Judicial Branch"; second, it "prevent[s] the Judiciary from encroaching into areas reserved for other branches." *Id.* at 678, 108 S. Ct. 2597.

Neither of these concerns is implicated here. Verizon does not appear to be arguing that the second of these concerns is threatened and, in fact, it is clear enough that the activity under § 512(h) poses no danger of encroachment or aggrandizement. Under § 512(h), the clerk carries out a

nondiscretionary duty that allows one private party to retrieve information from another private party. This rather passive, ministerial function by court personnel in no way resembles or impedes upon the authority of the Executive and Legislative Branches to pursue active investigation of possible civil or criminal wrongdoing. As the Supreme Court has noted, the "separation of powers 'left to each [Branch] power to exercise, in some respects, functions in their nature executive, legislative and judicial.'" *Mistretta v. United States*, 488 U.S. 361, 386, 109 S. Ct. 647, 102 L. Ed. 2d 714 (1989) (quoting *Myers v. United States*, 272 U.S. 52, 291, 47 S. Ct. 21 (1926) (Brandeis, J., dissenting)). Here, the minimal role of court personnel in issuing a § 512(h) subpoena "does not pose a sufficient threat of judicial intrusion into matters that are more properly within the Executive's [or Legislature's] authority to require that the Act be invalidated as inconsistent with Article III." *Morrison*, 487 U.S. at 683, 108 S. Ct. 2597.[11]

With respect to the first concern elucidated in *Morrison*, there is simply no basis to conclude that § 512(h) undermines the independence or institutional integrity of the Judicial Branch. Under § 512(h), the district court does not take sides in the copyright holder's request for the alleged infringer's name, but rather, through the clerk, serves as a passive, neutral instrument facilitating the attempt to retrieve the name. Furthermore, an Article III judge does not by virtue of the clerk's action become in any way invested in either the request for the alleged infringer's

---

[11] To the extent that a district court issuing a § 512(h) subpoena is properly understood to be exercising nothing other than a ministerial function, it is worth noting that the Supreme Court in *Morrison* held that the assumption of "essentially ministerial" powers by a special court under the Ethics in Government Act of 1978 did not impermissibly trespass upon the authority of the Executive Branch. *Id.* at 681, 108 S. Ct. 2597.

name or the potential copyright infringement case. The judge will still be able to approach any dispute over the information retrieval or the underlying copyright infringement in an entirely objective, unbiased fashion.

In short, given that the clerk only, and not a federal judge, issues a subpoena, § 512(h) does not "pose[ ] any threat to the 'impartial and independent federal adjudication of claims within the judicial power of the United States.' " *Id.* at 683, 108 S. Ct. 2597 (quoting *Commodity Futures Trading Comm'n v. Schor*, 478 U.S. 833, 850, 106 S. Ct. 3245, 92 L. Ed. 2d 675 (1986)). Any possible public perception that federal judges are being enlisted by copyright holders *ex parte* to investigate possible infringement would be based upon a complete misapprehension of how § 512(h) actually operates, and thus cannot provide a basis for striking down the provision.

There may be some merit, albeit quite limited, to Verizon's argument that § 512(h) foists a burden upon the Article III branch that could impede the judiciary's ability to perform its primary function--adjudication. Although no federal judge need allocate his or her time to issuing § 512(h) subpoenas, if, as Verizon hypothesizes, copyright holders start to present the clerks of the federal courts with tens of thousands of subpoena requests, some strain on the administrative resources of the judicial branch may result. But to date, that concern is entirely speculative, as no such barrage of requests has occurred. The statutory requirements for seeking a subpoena under § 512(h) serve, to some extent, to curtail the threat. Morever, Congress could ameliorate any additional burden on the courts by providing additional funding or resources. Verizon's challenge based on limited resources of the judiciary therefore cannot carry the day at this time.

In sum, § 512(h) does not place the Article III branch in a role inconsistent with that accorded to it under the Constitution. To the extent that the power of the judiciary is even implicated by the issuance of a subpoena under § 512(h), which assigns only a ministerial function to the clerk of the court, there are abundant analogues both in the criminal and civil contexts for judicial action in the absence of a pending federal case or controversy, including the close parallel of Rule 27.[12] And whatever authority is granted under § 512(h) presents neither a danger of encroachment nor some other threat to the institutional integrity and independence of the judiciary. Accordingly, and in light of the reluctance of the federal courts to declare an Act of

---

[12] Because the Court concludes that § 512(h) is constitutional on the grounds that it involves only a ministerial function by judicial personnel and is consonant with the role that federal courts have long played in other settings, the Court need not reach an alternate argument advanced by RIAA and the United States--that a case or controversy sufficient to provide a jurisdictional basis for the issuance of a subpoena inheres in the dispute between the copyright holder and the service provider over disclosing the alleged infringer's name. The Court notes, however, that when requesting a subpoena from the clerk of the court, a copyright holder need not assert that a disagreement over whether to provide the alleged infringer's name has emerged or will emerge. *See* 17 U.S.C. § 512(h)(1), (2). Indeed, the § 512(h) subpoena may constitute the copyright holder's first request for the alleged infringer's name, and conceivably the service provider will have no objections to disclosing the name (although, in this particular case, RIAA did make a pre-subpoena request for the name and Verizon did object). Thus, at the time of issuance, a § 512(h) subpoena will not necessarily be tethered to a present or even anticipated "adversary proceeding, involving a real, not a hypothetical, controversy" over providing the name. *Nashville, Chattanooga & St. Louis Ry. v. Wallace*, 288 U.S. 249, 259, 53 S. Ct. 345, 77 L. Ed. 730 (1933). Section § 512(h) is therefore not, as RIAA and the United States contend, analogous to 29 U.S.C. § 1132(c)(1), which allows an ERISA beneficiary to bring a civil action against a plan administrator for information only after the administrator has failed or refused to comply with a request for the information.

Congress unconstitutional, *see Mistretta*, 488 U.S. at 384, 109 S. Ct. 647,[13] and the substantial deference owed to Congress on copyright matters, *see Eldred v. Ashcroft*, 537 U.S. 186, 123 S. Ct. 769, 785, 788, 790, 154 L. Ed. 2d 683 (2003), Verizon's contention that § 512(h) is unconstitutional must fail.

III. SECTION 512(h) DOES NOT VIOLATE THE FIRST AMENDMENT

Verizon also contends that the subpoena authority in 512(h) violates the First Amendment rights of Internet users -- by piercing their anonymity -- both because it does not provide sufficient procedural protection for expressive and associational rights and because it is overbroad and sweeps in protected expression. Although these are certainly important considerations, the Court concludes that § 512(h) does not offend the First Amendment.

---

[13] Verizon cites Justice Scalia's dissenting opinion in *Morrison* for the proposition that deference is not owed to Congress in assessing the constitutionality of a statute where separation of powers issues are at stake. But one of the factors motivating Justice Scalia's conclusion that deference was unwarranted in *Morrison* was the fact that, in that case, the "political branches [were] ... in disagreement" as to the constitutionality of the statute at issue, and thus neither branch could "be presumed correct." *Morrison*, 487 U.S. at 705, 108 S. Ct. 2597 (Scalia, J., dissenting). Here, of course, the Executive Branch has now intervened in this case to defend the constitutionality of the statute, and hence the political branches are in full accord. Moreover, in *Mistretta*, which followed *Morrison* and involved separation of powers issues concerning the independence and integrity of the judiciary, the Supreme Court stated unequivocally: "'When this Court is asked to invalidate a statutory provision that has been approved by both Houses of the Congress and signed by the President, particularly an Act of Congress that confronts a deeply vexing national problem, it should only do so for the most compelling constitutional reasons.'" 488 U.S. at 384, 109 S. Ct. 647 (quoting *Bowsher v. Synar*, 478 U.S. 714, 736, 106 S. Ct. 3181, 92 L. Ed. 2d 583 (1986) (opinion concurring in judgment)).

A. Verizon Has Standing to Assert the First Amendment Rights of its Subscribers

A "plaintiff generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights and interests of third parties." *Warth v. Seldin*, 422 U.S. 490, 499, 95 S. Ct. 2197, 45 L. Ed. 2d 343 (1975).[14] This rule prevents "premature interpretations of statutes in areas where their constitutional application might be cloudy" and "assures the court that the issues before it will be concrete and sharply presented." *Sec'y of State of Maryland v. Joseph H. Munson Co.*, 467 U.S. 947, 955, 104 S. Ct. 2839, 81 L. Ed. 2d 786 (1984). The Supreme Court "has altered its traditional rules of standing to permit -- in the First Amendment area -- 'attacks on overly broad statutes with no requirement that the person making the attack demonstrate that his own conduct could not be regulated by a statute drawn with the requisite narrow specificity.'" *Broadrick v. Oklahoma*, 413 U.S. 601, 612, 93 S. Ct. 2908, 37 L. Ed. 2d 830 (1973) (quoting *Dombrowski v. Pfister*, 380 U.S. 479, 486, 85 S. Ct. 1116, 14 L. Ed. 2d 22 (1965)). As the Supreme Court stated in *Broadrick:*

> Litigants, therefore, are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court

---

[14] Although RIAA does not directly challenge Verizon's standing to assert the First Amendment rights of its subscribers, the Court nonetheless must determine whether Verizon has standing to bring these claims. "The federal courts are under an independent obligation to examine their own jurisdiction, and standing 'is perhaps the most important of [the jurisdictional] doctrines.'" *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231, 110 S. Ct. 596, 107 L. Ed. 2d 603 (1990) (quoting *Allen v. Wright*, 468 U.S. 737, 750, 104 S. Ct. 3315, 82 L. Ed. 2d 556 (1984)).

> to refrain from constitutionally protected speech or expression.

Id.; accord Joseph H. Munson Co., 467 U.S. at 956, 104 S. Ct. 2839 (party may assert First Amendment overbreadth challenge "of another without regard to the ability of the other to assert his own claim"). Thus, even though Verizon's two subscribers here could arguably assert their own rights,[15] Verizon nonetheless may assert a First Amendment challenge on their behalf.

Although Verizon's First Amendment rights are not directly implicated by RIAA's subpoenas, "[f]acial challenges to overly broad statutes are allowed not primarily for the benefit of the litigant, but for the benefit of society -- to prevent the statute from chilling the First Amendment rights of other parties not before the court." *Joseph H. Munson Co.*, 467 U.S. at 958, 104 S. Ct. 2839.

> Even where a First Amendment challenge could be brought by one actually engaged in protected activity, there is a possibility that, rather than risk punishment for his conduct in challenging the statute, he will refrain from engaging further in the protected activity. Society as a whole then would be the loser. Thus, when there is a danger of chilling free speech, the concern that constitutional adjudication be avoided whenever possible may be outweighed by society's interest in having the statute challenged.

---

[15] The alleged infringers could assert their own First Amendment rights, while still protecting their anonymity, as "John Doe" litigants. Verizon has now notified both subscribers of RIAA's subpoenas and allegations of copyright infringement.

Id. at 956, 104 S. Ct. 2839. A plaintiff's "ability to serve that function has nothing to do with whether or not its own First Amendment rights are at stake." *Id.* at 958, 104 S. Ct. 2839.

Verizon is, moreover, an adequate advocate to assert the First Amendment rights of its subscribers. The relationship between an Internet service provider and its subscribers is the type of relationship courts have found will ensure that issues will be "concrete and sharply presented." Verizon has a vested interest in vigorously protecting its subscribers' First Amendment rights, because a failure to do so could affect Verizon's ability to maintain and broaden its client base. The Supreme Court has recognized third-party standing in similar business/client relationships. *See Virginia v. American Booksellers Assoc.*, 484 U.S. 383, 392-93, 108 S. Ct. 636, 98 L. Ed. 2d 782 (1988) (bookstores may raise First Amendment rights on behalf of booksellers); *Joseph H. Munson Co.*, 467 U.S. at 958, 104 S. Ct. 2839 (professional fundraiser may assert First Amendment rights of its client charities); *Dep't of Labor v. Triplett*, 494 U.S. 715, 720, 110 S. Ct. 1428, 108 L. Ed. 2d 701 (1990) ("A restriction upon the fees a lawyer may charge that deprives the lawyer's prospective client of a due process right to obtain legal representation falls squarely within this principle."); *Craig v. Boren*, 429 U.S. 190, 194-97, 97 S. Ct. 451, 50 L. Ed. 2d 397 (1976) (beer vendor may assert equal protection claims of males not allowed to purchase beer until they turn 21); *see also Broadrick*, 413 U.S. at 612, 93 S. Ct. 2908 ("Overbreadth attacks [raised by third-parties] have also been allowed where the Court thought rights of association were ensnared in statutes which, by their broad sweep, might result in burdening innocent associations."). Verizon's relationship with its client subscribers is the kind of relationship that

warrants allowing Verizon to assert a First Amendment challenge on their behalf.[16]

B. The First Amendment Protects Anonymous Expression on the Internet

The Supreme Court has recognized a right of anonymity within the First Amendment. *Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 200, 119 S. Ct. 636, 142 L. Ed. 2d 599 (1999) (invalidating, on First Amendment grounds, a Colorado statute that required initiative petitioners to wear identification badges); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357, 115 S. Ct. 1511, 131 L. Ed. 2d 426 (1995) (overturning Ohio law that prohibited distribution of campaign literature without name and address of the person issuing the literature; "anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent"); *Talley v. California*, 362 U.S. 60, 65, 80 S. Ct. 536, 4 L. Ed. 2d 559 (1960) (invalidating California statute prohibiting distribution of handbills without name and address of preparer).[17] Courts have also recognized that the protections of the First Amendment reach expression on the Internet. *See, e.g., Reno v. ACLU*, 521 U.S. 844, 870, 117 S. Ct. 2329, 138 L. Ed. 2d 874

---

[16] The Court is also aided in this case by the submissions of *amici* representing the interests of Internet users.

[17] Courts have acknowledged some limitations on the subpoena power when its invocation affects First Amendment rights involving anonymity. *See, e.g., NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 461, 78 S. Ct. 1163, 2 L. Ed. 2d 1488 (1958) (discussing First Amendment implications of civil subpoena to disclose membership list); *Doe v. 2TheMart.Com Inc.*, 140 F. Supp. 2d 1088, 1091 (W.D. Wash. 2001) (addressing First Amendment rights when corporation served subpoena on ISP to obtain identity of anonymous shareholders in derivative action); *Los Angeles Memorial Coliseum Comm'n v. Nat'l Football League*, 89 F.R.D. 489 (C.D.Cal.1981) (discussing First Amendment implications of civil subpoena to disclose names of confidential journalistic sources).

(1997) ("Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates further than it could from any soapbox."); *2TheMart.Com*, 140 F. Supp. 2d at 1092 ("First Amendment protections extend to speech via the Internet.").

An individual's anonymity may be important for encouraging the type of expression protected by the First Amendment. "The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible." *McIntyre*, 514 U.S. at 341-42, 115 S. Ct. 1511. Indeed, "quite apart from any threat of persecution, an advocate may believe her ideas will be more persuasive if her readers are unaware of her identity." *Id.* at 342, 115 S. Ct. 1511. As stated in *Talley*, "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." 362 U.S. at 64, 80 S. Ct. 536. Hence, several lower court cases have found that First Amendments rights, particularly the right to anonymity, extend to expression on the Internet. *See, e.g., 2TheMart.Com*, 140 F. Supp. 2d at 1097 ("the constitutional rights of Internet users, including the right to speak anonymously, must be carefully safeguarded"); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1033 (D.N.M. 1998) (striking law "that prevents people from communicating and accessing information anonymously"); *Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (recognizing "legitimate and valuable right to participate in online forums anonymously or pseudonymously").

But when the Supreme Court has held that the First Amendment protects anonymity, it has typically done so in cases involving core First Amendment expression. *See, e.g., Watchtower Bible, Tract Society of New York, Inc. v. Village of*

Stratton, 536 U.S. 150, 153, 122 S. Ct. 2080, 153 L. Ed. 2d 205 (2002) (striking down ordinance requiring permit for door-to-door advocacy "not only as it applies to religious proselytizing, but also to anonymous political speech and the distribution of handbills"); *Buckley*, 525 U.S. at 199, 119 S. Ct. 636 (striking down petition circulation rule requiring petitioners to be registered voters because "that endeavor . . . of necessity involves . . . the expression of a desire for political change"); *McIntyre*, 514 U.S. at 346, 115 S. Ct. 1511 ("the speech in which Mrs. McIntyre engaged -- handing out leaflets in the advocacy of a politically controversial viewpoint -- is the essence of First Amendment expression"). As the Supreme Court has explained, "[t]he First Amendment affords the broadest protection to such political expression in order 'to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'" *Id.* at 346, 115 S. Ct. 1511 (quoting *Roth v. United States*, 354 U.S. 476, 484, 77 S. Ct. 1304, 1 L. Ed. 2d 1498 (1957)). "When a law burdens core political speech, we apply 'exacting scrutiny,' and we uphold the restriction only if it is narrowly tailored to serve an overriding state interest." *Id.* at 347, 115 S. Ct. 1511.

The DMCA, however, does not directly impact core political speech, and thus may not warrant the type of "exacting scrutiny" reserved for that context. Section 512(h) deals strictly with copyright infringement. Verizon concedes, as it must, that there is no First Amendment defense to copyright violations. The "Supreme Court . . . has made it unmistakably clear that the First Amendment does not shield copyright infringement." *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000); *see Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 568, 105 S. Ct. 2218, 85 L. Ed. 2d 588 (1985) (rejecting First Amendment challenge to copyright infringement action); *Zacchini v. Scripps-Howard*, 433 U.S. 562, 574-78, 97 S.

Ct. 2849, 53 L. Ed. 2d 965 (1977). In other words, "the First Amendment is not a license to trammel on legally recognized rights in intellectual property." *In re Capital Cities/ABC, Inc.*, 918 F.2d 140, 143 (11th Cir. 1990) (quotations omitted). Indeed, copyrights serve as important incentives to encourage and protect expression: "the Framers intended copyright itself to be the engine of free expression." *Eldred*, 123 S. Ct. at 788 (quoting *Harper & Row*, 471 U.S. at 558, 105 S. Ct. 2218). "By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." *Id.* Nonetheless, the Court concludes for present purposes that there is some level of First Amendment protection that should be afforded to anonymous expression on the Internet, even though the degree of protection is minimal where alleged copyright infringement is the expression at issue.

C. § 512(h) Provides Sufficient Safeguards to Protect Internet Users' Rights

Verizon maintains that the DMCA does not provide adequate safeguards to protect Internet users' rights of expression and association. In this regard, Verizon relies heavily on the Supreme Court's decision in *Blount v. Rizzi*, 400 U.S. 410, 91 S. Ct. 423, 27 L. Ed. 2d 498 (1971), which overturned a federal statute authorizing prior restraint and censorship of obscene materials sent through the mail. The Court in *Blount* held that "the line between speech unconditionally guaranteed and speech which may legitimately be regulated . . . is finely drawn," and thus "[t]he separation of legitimate from illegitimate speech calls for sensitive tools." *Id.* at 417, 91 S. Ct. 423 (quoting *Speiser v. Randall*, 357 U.S. 513, 525, 78 S. Ct. 1332, 2 L. Ed. 2d 1460 (1958)). The strictures in *Blount* and its progeny, however, do not apply outside the obscenity realm; moreover, even if they did, the DMCA contains adequate safeguards to ensure

that the First Amendment rights of Internet users will not be curtailed.

Blount struck down a statute that authorized the Postmaster General to halt the use of the mails for commerce in allegedly obscene materials and permitted detention of mail pending resolution of an obscenity determination.

> Since § 4006 on its face, and § 4007 as applied, are procedures designed to deny use of the mails to commercial distributors of obscene literature, those procedures violate the First Amendment unless they include built-in safeguards against curtailment of constitutionally protected expression, for Government is not free to adopt whatever procedures it pleases for dealing with obscenity . . . without regard to the possible consequences for constitutionally protected speech. Rather, the First Amendment requires that procedures be incorporated that ensure against the curtailment of constitutionally protected expression, which is often separate from obscenity only by a dim and uncertain line.

400 U.S. at 416, 91 S. Ct. 423 (citations omitted). Because the government was censoring speech and regulating obscenity, the Court "insist[ed] that regulations of obscenity scrupulously embody the most rigorous procedural safeguards." *Id.* "[T]he fatal flaw of the [statute's] procedure," the Court explained, was that it "fail[ed] to require that the Postmaster General seek to obtain a prompt judicial determination of the obscenity of the material." *Id.* at 418, 91 S. Ct. 423.

The Supreme Court's decision in *Blount* cannot be read as broadly as Verizon would like. The statute challenged in *Blount* authorized government censorship and prior restraint

of allegedly obscene material sent through the mail, without any judicial determination of obscenity. In such circumstances, the Court emphasized, "the censor's business is to censor." *Id.* at 419, 91 S. Ct. 423. "The teaching of our cases is that, because only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint.'" *Id.* (quoting *Freedman v. Maryland*, 380 U.S. 51, 58, 85 S. Ct. 734, 13 L. Ed. 2d 649 (1965)). The Court emphasized that "it is vital that prompt judicial review on the issue of obscenity--rather than merely probable cause -- be assured on the Government's initiative before the severe restrictions in [the statute] are invoked." *Id.* at 420, 91 S. Ct. 423.

Unlike the statute in *Blount*, however, the DMCA neither authorizes governmental censorship nor involves prior restraint of potentially protected expression. Section 512(h) merely allows a private copyright owner to obtain the identity of an alleged copyright infringer in order to protect constitutionally-recognized rights in creative works; it does not even directly seek or restrain the underlying expression (the sharing of copyrighted material). Thus, the DMCA does not regulate protected expression or otherwise permit prior restraint of protected speech. It only requires production of the identity of one who has engaged in unprotected conduct sharing copyrighted material on the Internet. The statute in *Blount*, in contrast, authorized both prior restraint and censorship by the government -- a far more "severe restriction" on First Amendment rights. Content-based prior restraint of expressive activity, the Supreme Court has held, warrants the strictest scrutiny known to First Amendment jurisprudence. *See New York Times Co. v. United States*, 403 U.S. 713, 714, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971) (per curiam) ("'Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its

constitutional validity.'") (quoting *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70, 83 S. Ct. 631, 9 L. Ed. 2d 584 (1963)). The DMCA places no limits on protected activity; it governs unprotected copyright piracy, and § 512(h) reaches only the identity of the subscriber (already known to the service provider), not any underlying expression. Moreover, the content of § 512(h) is not obscenity but copyright legislation, where "[t]he wisdom of Congress' action . . . is not within [the Court's] province to second guess." *Eldred*, 123 S. Ct. at 790.

The Supreme Court has not extended *Blount's* requirements of "built-in safeguards" and judicial review beyond the obscenity context,[18] and lower federal courts have declined to apply *Blount* and its progeny in other contexts.[19] Because the DMCA does not address obscenity

---

[18] The application of *Blount* has been limited to obscenity settings. *See, e.g., FW/PBS v. City of Dallas*, 493 U.S. 215, 239, 110 S. Ct. 596, 107 L. Ed. 2d 603 (1990) (licensing ordinance for adult entertainment industry); *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 561, 95 S. Ct. 1239, 43 L. Ed. 2d 448 (1975) (sex and nudity in play); *Paris Adult Theatre v. Slaton*, 413 U.S. 49, 55, 93 S. Ct. 2628, 37 L. Ed. 2d 446 (1973) (Georgia obscenity law relating to films in theaters); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 368, 91 S. Ct. 1400, 28 L. Ed. 2d 822 (1971) (forfeiture of obscene photographs found in luggage); *United States v. Reidel*, 402 U.S. 351, 359, 91 S. Ct. 1410, 28 L. Ed. 2d 813 (1971) ("if government chooses a system of prior restraints as an aid to its goal of proscribing obscenity, the system must be designed to minimize impact on speech which is constitutionally protected") (Marshall, J., concurring). In a First Amendment challenge involving a labor context, the Supreme Court--citing *Blount*--explained that "[i]n other First Amendment contexts, of course, we have required swift judicial review of the challenged governmental action. In this context, we do not believe that such special judicial procedures are necessary." *Chicago Teachers Union v. Hudson*, 475 U.S. 292, 307 n. 20, 106 S. Ct. 1066, 89 L. Ed. 2d 232 (1986).

[19] *See, e.g., Cannabis Action Network, Inc. v. City of Gainesville*, 231 F.3d 761, 775 (11th Cir. 2000) (*Blount* line of cases "predominantly involved censorship"of obscene materials); *O'Connor v. City and County of Denver*,

and does not censor or otherwise authorize prior restraint of expression, the Court finds Verizon's reliance on *Blount* is misplaced.

Even if such safeguards were required, however, the DMCA includes sufficient procedures to prevent any substantial encroachment on the First Amendment rights of Internet users. Before a copyright owner (or its agent) can obtain a § 512(h) subpoena, for example, one must have a "good faith belief" that the use of copyrighted material is not authorized by the owner. 17 U.S.C. § 512(c)(3)(A)(v). Moreover, the DMCA requires a copyright owner to submit

> a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

Id. § 512(h)(2)(c). The DMCA also requires a person seeking a subpoena to state, under penalty of perjury, that he is authorized to act on behalf of the copyright owner. *Id.* § 512(c)(3)(A)(vi). These provisions provide substantial protection for Internet users against baseless or abusive subpoenas.[20] In fact, the statute contains an important

---

894 F.2d 1210, 1223 (10th Cir. 1990) ("The *Freedman* requirements [adopted by the Court in *Blount*] are limited to prior restraints on protected expression."); *United States v. Outpost Development Corp.*, 369 F. Supp. 399, 402 (C.D.Cal.1973) ("[w]e read *Blount* as being applicable to questions involving alleged obscenity, but not to alleged fraudulent schemes"); *Lynch v. Blount*, 330 F. Supp. 689, 694 (S.D.N.Y.1971) ("We think the safeguards defined in *Blount* for obscenity cases are wholly inappropriate, unnecessary and inapplicable to the field of commercial fraud.").

[20] Congress specifically enacted these procedural requirements to prevent mistakes and abuse. *See* S.Rep. No. 105-190, at 9 (explaining that the DMCA contains "important procedural protections for individual Internet users to ensure that they will not be mistakenly denied access to the World Wide Web").

disincentive for false representations, thereby further protecting against abusive or harassing subpoenas. *See id.* § 512(f) (any person who "knowingly materially misrepresents" that activity is infringing "shall be liable for damages, including costs and attorneys' fees, incurred by the alleged infringer" as a result of the misrepresentation). With all these protections, it is unlikely that § 512(h) will require disclosure, to any significant degree, of the identity of individuals engaged in protected anonymous speech, as opposed to those engaged in unprotected copyright infringement.

Verizon asserts that, under the DMCA, a copyright owner does not have to demonstrate that the allegation of copyright infringement could withstand a motion to dismiss. However, in order to obtain a subpoena, the copyright owner must, in effect, plead a prima facie case of copyright infringement. *See Feist Publ'ns, Inc. v. Rural Tel. Svc. Co.*, 499 U.S. 340, 361, 111 S. Ct. 1282, 113 L. Ed. 2d 358 (1991) (the elements of a prima facie case of copyright infringement are "(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original"); *accord, Lulirama, Ltd. v. Axcess Broadcast Svcs.*, 128 F.3d 872, 884 (5th Cir. 1997). Under § 512, one must assert ownership of an exclusive copyright, § 512(c)(3)(A)(i), and a good faith belief that the use of copyrighted material is not authorized, § 512(c)(3)(A)(v). In other words, the subpoena notification must establish ownership and unauthorized use -- a prima facie case of copyright infringement.[21]

---

[21] Although the standard for obtaining a § 512(h) subpoena differs somewhat from the standard for obtaining a subpoena through the more traditional procedure governed by Fed. R. Civ. P. 11, the difference is not substantial. Under § 512(c)(3)(A)(v), a copyright owner must have a "good faith belief" that the use of the copyrighted material is not authorized. Under Rule 11, a party or attorney can be sanctioned absent

Lastly, the DMCA provides that the Federal Rules of Civil Procedure govern the issuance, service, enforcement, and compliance of subpoenas. 17 U.S.C. § 512(h)(6). Hence, access to the courts and the judicial supervision Verizon urges to protect Internet users is available. Service providers or their subscribers, for example, can employ Fed.R.Civ.P. 45 to object to, modify or move to quash a subpoena, or even to seek sanctions. *See, e.g.*, Fed. R. Civ. P. 45(c)(1) (authorizing sanctions for overbroad, burdensome, or vexatious subpoenas). This adds yet another layer of protection for Internet users.[22] Thus, in sum, the Court rejects Verizon's contention that § 512 does not provide sufficient safeguards or judicial supervision to protect Internet users' First Amendment rights, including anonymity.

---

an "objective" basis that the claim was sound. *See Tahfs v. Proctor*, 316 F.3d 584, 594 (6th Cir. 2003) (requiring objective basis for claims under Rule 11); *Byrne v. Nezhat*, 261 F.3d 1075, 1105-06 (11th Cir. 2001) (same). Both procedures allow for sanctions for any baseless or meritless claims.

[22] These provisions under § 512 are precisely the type of procedural requirements other courts have imposed--in non-copyright cases -- to compel a service provider to reveal the identity of anonymous Internet users. *See Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 578-80 (N.D.Cal.1999) (in trademark dispute against anonymous person, court required plaintiff to identify person with specificity, identify all steps taken to locate elusive person, establish that suit could withstand motion to dismiss, and show "probable cause [as] a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong"); *Doe v. 2TheMart.Com, Inc.*, 140 F. Supp. 2d. at 1095 (to obtain subpoena to identify anonymous poster of criticism of corporation, party must show it was acting in good faith and not for an improper purpose, that information directly related to core claim, and that information was unavailable from any other source); *In re Subpoena Duces Tecum to America Online, Inc.*, 2000 WL 1210372, * 8 (Va. Cir. Ct. Jan.31, 2000) (to obtain identity of anonymous Internet users, court required that "the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable" and that information sought "is centrally needed to advance that claim").

D. Section 512(h) Is Not Overbroad

Verizon claims that the § 5121(h) subpoena authority is substantially overbroad and will chill protected anonymous speech and association. As explained earlier, the overbreadth doctrine permits facial challenges to statutes on the ground that the statute or regulation reaches constitutionally protected speech of parties not before the court. *Broadrick*, 413 U.S. at 612-15, 93 S. Ct. 2908. If a statute is substantially overbroad, and thus sweeps within its proscriptions a good amount of protected expression, the statute is unconstitutional. The doctrine is predicated on "a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression." *Id.* at 612, 93 S. Ct. 2908.

The scope of § 512(h) may impact some protected expression and association, in that the threat of a subpoena under the DMCA, and the resulting disclosure of identity, could discourage some Internet users from otherwise protected activity. It is also possible that a copyright owner could mistakenly pursue, and obtain, the identity of an anonymous Internet user who was not, in actuality, infringing copyrighted materials. Yet, "[t]o prevail in a facial challenge, however, it is not enough for a plaintiff to show 'some' overbreadth. Rather, the overbreadth of a statute must not only be real, but substantial as well." *Ashcroft v. ACLU*, 535 U.S. 564, 584, 122 S. Ct. 1700, 152 L. Ed. 2d 771 (2002) (citations omitted); *Houston v. Hill*, 482 U.S. 451, 458, 107 S. Ct. 2502, 96 L. Ed. 2d 398 (1987) ("Only a statute that is substantially overbroad may be invalidated on its face."). The § 512(h) subpoena authority hardly amounts to a real or substantial threat to protec ed expression. Indeed, Verizon has not come forward with any evidence that in the five years since the DMCA was enacted, § 512(h)

subpoenas have been used to identify anyone but Internet users engaging in copyright infringement.[23]

Verizon also portends that § 512(h) could be used by "cyberstalkers" to issue fraudulent subpoenas to obtain identifying information (such as phone numbers and addresses) about people they meet in Internet chat rooms. Of course, this anonymity issue, although perhaps somewhat related to a First Amendment expressive interest, is generated more by safety concerns. As such, it may be more properly considered as a policy argument against broad subpoena authority, and therefore a matter for Congress rather than this Court. But in any event, requirements in the DMCA should prevent such speculation from ever becoming a reality. In order to get a subpoena, one must identify the material claimed to be infringing, and information reasonably sufficient to permit the service provider to locate the material. *See* § 512(c)(3)(A)(iii). Likewise, § 512(c)(3)(A)(ii) requires identification of the online site where the copyrighted works are claimed to be infringed. Although conceivably one could falsify such information in a subpoena, the information is also easily verifiable by service providers, who can provide an additional check against fraudulent conduct. In fact, the remedial provisions of the DMCA, including the right to damages for misrepresentation, attorneys fees, contempt

---

[23] Verizon highlights an incident involving a notice to an Internet service provider alleging possible copyright infringement of a Harry Potter film. The allegedly infringing work turned out to be a child's book report, which the "robotic" software could not distinguish from the copyrighted work. However, the copyright owner did not issue a § 512(h) subpoena, but merely notified the service provider by letter of the alleged infringement. Such mistakes are possible using evolving technology, but there is nothing to suggest they will cause substantial chilling of expression on the Internet.

sanctions and even the possibility of criminal perjury charges, should deter potential stalkers.

The risk of cyberstalking and any accompanying impact on expressive interests, then, is minimal. As the Supreme Court has explained, "the mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge." *Taxpayers for Vincent*, 466 U.S. at 800, 104 S. Ct. 2118. "Although such laws, if too broadly worded, may deter protected speech to some unknown extent, there comes a point where that effect -- at best a prediction -- cannot, with confidence, justify invalidating a statute on its face." *Ferber*, 458 U.S. at 770, 102 S. Ct. 3348. Again, it is noteworthy that although it has been nearly five years since § 512 came into effect, there is nothing in the record to indicate that the DMCA subpoena authority has been used for stalking or other fraudulent purposes. Hence, while conceivable, Verizon's cyberstalking scenario is unlikely, and the DMCA cannot be found unconstitutionally overbroad on such a thin reed of speculation. *See Taxpayers for Vincent*, 466 U.S. at 800 n. 19, 104 S. Ct. 2118 ("We have never held that a statute should be held invalid on its face merely because it is possible to conceive of a single impermissible application, and in that sense a requirement of substantial overbreadth is already implicit in the doctrine.") (quoting *Broadrick*, 413 U.S. at 630, 93 S. Ct. 2908 (Brennan, J., dissenting)); *Ferber*, 458 U.S. at 771, 102 S. Ct. 3348 ("[A] law should not be invalidated for overbreadth unless it reaches a substantial number of impermissible applications.").

The Supreme Court has emphasized repeatedly that "where a statute regulates expressive conduct, the scope of the statute does not render it unconstitutional unless its overbreadth is not only real, but substantial as well, judged in relation to the statute's plainly legitimate sweep." *Osborne*

v. Ohio, 495 U.S. 103, 112, 110 S. Ct. 1691, 109 L. Ed. 2d 98 (1990). Any overbreadth resulting from § 512(h) that arguably chills First Amendment expression or association is neither "real" nor "substantial" in relation to the DMCA's "plainly legitimate sweep" of identifying copyright infringers. The extent of copyright infringement and piracy of intellectual property over the Internet, on the other hand, is well-recognized and "has reached epidemic proportions." *United States v. Elcom, Ltd.*, 203 F. Supp. 2d 1111, 1132 (N.D.Cal.2002). The recording industry has suffered substantial losses due to Internet piracy Whatever marginal impact the DMCA subpoena authority may have on the expressive or anonymity rights of Internet users, then, is vastly outweighed by the extent of copyright infringement over the Internet through peer-to-peer file sharing, which is the context of the legitimate sweep of § 512(h).

The DMCA does not regulate expression, and § 512(h) is not directed at the suppression of expression. Indeed, Congress enacted the DMCA in part to *spur* and *promote* expression, not suppress it. Congress was concerned that "copyright owners [would] hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy." S. Rep. No. 105-190, at 8 (1998). The ability to copyright, in fact, is "the engine of free expression." *Eldred*, 123 S. Ct. at 788 (quoting *Harper & Row*, 471 U.S. at 558, 105 S. Ct. 2218). Hence, the DMCA *fosters* speech by helping artists, musicians, and authors protect their creative works, in turn encouraging further expression.

The Supreme Court has cautioned that application of the overbreadth doctrine "is, manifestly, strong medicine." *Broadrick*, 413 U.S. at 613, 93 S. Ct. 2908. The doctrine is therefore employed "with hesitation, and then 'only as a last resort.'" *Ferber*, 458 U.S. at 769, 102 S. Ct. 3348 (quoting

Broadrick, 413 U.S. at 613, 93 S. Ct. 2908). "[T]here must be a *realistic danger* that the statute itself will *significantly compromise* recognized First Amendment protections of parties not before the Court for it to be facially challenged on overbreadth grounds." *Taxpayers for Vincent*, 466 U.S. at 801, 104 S. Ct. 2118 (emphasis added). Verizon simply has not shown that the subpoena authority under § 512(h) is so overbroad that it sweeps a substantial amount of protected expression within the DMCA's proscriptions. Verizon's bald speculation of mistakes, abuse or harassment that has yet to occur to any degree (let alone to any substantial degree) since the statute was enacted is simply not enough. "[J]udged in relation to the statute's plainly legitimate sweep," and in light of the extent of copyright piracy over the Internet, any impact on expressive and associational rights on the Internet is negligible.

Ultimately, Verizon suggests that even if § 512(h) is not found facially unconstitutional, it should nonetheless be construed narrowly so as to avoid serious First Amendment issues. "When the validity of an act of Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will ascertain whether a construction of the statute is fairly possible by which the question may be avoided." *Public Citizen v. Dep't of Justice*, 491 U.S. 440, 465-66, 109 S. Ct. 2558, 105 L. Ed. 2d 377 (1989) (citation omitted). Hence, "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Id.* at 466, 109 S. Ct. 2558.

To begin with, this Court has already determined in its *First Subpoena Decision* that the construction of § 512(h) Verizon proposes is not plausible given the statutory

language, context, purpose and legislative history, and thus would be "plainly contrary to the intent of Congress." Moreover, before this constitutional avoidance doctrine can be applied, a Court must first be faced with a "grave" constitutional question, *AAPS v. Clinton*, 997 F.2d 898, 906 (D.C. Cir. 1993), or a "formidable constitutional difficult[y]," *Public Citizen*, 491 U.S. at 466, 109 S. Ct. 2558. Here, § 512(h) does not present a grave or formidable constitutional problem. As explained above, the Court rejects Verizon's First Amendment challenge to § 512(h).[24] "[T]he Court need not apply ... the doctrine ... where a constitutional question, while lacking an obvious answer, does not lead a majority gravely to doubt that the statute is constitutional." *Almendarez-Torres v. United States*, 523 U.S. 224, 239, 118 S. Ct. 1219, 140 L. Ed. 2d 350 (1998).

Even if the Court were presented with such grave doubts, moreover, Verizon's proposed construction of the statute would not eliminate the constitutional problem, but rather would only reduce it. The Court has construed § 512(h) as applying to all service providers under the DMCA, including those falling within the conduit functions under subsection (a). Verizon would construe § 512(h)'s subpoena power to apply only to subsection (c), where the subscriber stores his allegedly infringing material on the service provider's system. But Internet users who fall within subsection (c) have anonymity interests identical to users within subsection (a), and hence would be susceptible to the same chilling of expressive and associational rights asserted by Verizon. Thus, Verizon's construction would only mean

---

[24] Constitutional avoidance does not apply to Verizon's Article III challenge, as no limiting construction of § 512(h) would cure that alleged constitutional defect--the alleged "case or controversy" deficiency pertains to *any* subpoena, whether addressed to a subsection (a) or subsection (c) service provider.

that fewer users would have their First Amendment interests impacted -- the same alleged constitutional problem would persist to some degree.

"The principle . . . is a categorical one: as between two possible interpretations of a statute, by one of which it would be unconstitutional and by the other valid, our plain duty is to adopt that which will save the Act." *Rust v. Sullivan*, 500 U.S. 173, 190, 111 S. Ct. 1759, 114 L. Ed. 2d 233(1991) (quoting *Blodgett v. Holden*, 275 U.S. 142, 148, 48 S. Ct. 105, 72 L. Ed. 206 (1927)). But reading § 512(h) as applying only to subsection (c) users does not eliminate Verizon's alleged constitutional problem -- it only reduces it -- and thus will not "save" the DMCA. If the subpoena authority under § 512(h) chills expression and association, it does so as applied to both subsection (c) users and subsection (a) users. Hence, not only is the narrow construction urged by Verizon not a plausible one to which § 512(h) is "genuinely susceptible," as this Court has previously found, *see First Subpoena Decision*, 240 F. Supp. 2d at 30-39, but it would not save § 512(h) from the alleged constitutional infirmity in any event.

In the end, Verizon's customers should have little expectation of privacy (or anonymity) in infringing copyrights. Subscribers to Verizon's Internet services are put on clear notice that they cannot use Verizon's service or network to infringe copyrights. *See* Verizon Online Terms of Service, *http://www.verizon.net/policies/popups/internetaa popup.asp*. In fact, as part of its corporate policy, Verizon alerts its subscribers at the outset that it will "disclose individual customer information to an outside entity ... when Verizon is served with valid legal process for customer information." *See* Verizon Privacy Principles, *http://www22.verizon.com/About/Privacy/genpriv*. And if an individual subscriber opens his computer to permit others,

through peer-to-peer filesharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world. *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (no expectation of privacy where user has opened files up on home computer to anyone who wants to receive them).

IV. VERIZON'S STAY REQUEST

Verizon emphasizes that both subpoena actions are test cases raising issues of first impression, and urges the Court to stay its rulings on both matters pending appeal. Although the Court does not dispute Verizon's characterization of these subpoena cases, novelty of issues alone does not entitle a litigant to a stay pending appeal. Applying the well-established standards in this Circuit, Verizon's request for a stay pending appeal must be denied.

A. Standard for a Stay

To obtain a stay pending appeal, Verizon "must show (1) that it has a substantial likelihood of success on the merits; (2) that it will suffer irreparable injury if the stay is denied; (3) that issuance of the stay will not cause substantial harm to other parties; and (4) that the public interest will be served by issuance of the stay." *United States v. Philip Morris Inc.*, 314 F.3d 612, 617 (D.C. Cir. 2003) (citing *Washington Metro. Area Transit Comm'n v. Holiday Tours. Inc.*, 559 F.2d 841, 843 (D.C. Cir. 1977)). "These factors interrelate on a sliding scale and must be balanced against each other." *Serono Labs., Inc. v. Shalala*, 158 F.3d 1313, 1318 (D.C. Cir. 1998); *CityFed Fin. Corp. v. Office of Thrift Supervision*, 58 F.3d 738, 747 (D.C. Cir. 1995) ("If the arguments for one factor are particularly strong, [a stay] may issue even if the arguments in other areas are rather weak."). On a motion for stay, "it is the movant's obligation to justify the court's exercise of such

an extraordinary remedy." *Cuomo v. U.S. Nuclear Reg. Comm'n*, 772 F.2d 972, 978 (D.C. Cir. 1985).[25] Although there may be a temptation to conclude that a stay is warranted in this "test" case to enable the Court of Appeals to consider issues arguably of first impression, Verizon in fact has a heavy burden to justify an entitlement to this "extraordinary remedy."

B. Likelihood of Success on the Merits

Verizon's likelihood of success on the merits of its claims, both statutory and constitutional, is minimal. In the *First Subpoena Decision*, the Court concluded "that the subpoena power in 17 U.S.C. § 512(h) applies to all Internet service providers within the scope of the DMCA, not just those service providers storing information on a system or network at the direction of a user." 240 F. Supp. 2d at 26. Verizon argues that the Court's central reliance on the definition of the term "service provider" is "misplaced." However, the Court followed well-accepted canons of statutory construction in applying § 512(k)'s broad definition of "service provider" to the subpoena authority under § 512(h). First and foremost, the plain language of the statute's definition provision in subsection (k) mandates this result. It is only by dismissing the subsection (k) definition of "service provider" altogether that Verizon can contend otherwise. But there is no basis for ignoring that clear, governing definitional language. Where a statute "unambiguously uses a statutorily defined term, that

---

[25] Although presenting a serious legal issue on appeal may weigh in favor of a stay, the movant still must demonstrate that the balance of harms strongly favors such relief. *See Nat'l Ass'n of Farmworkers v. Marshall*, 628 F.2d 604, 616 (D.C. Cir. 1980); *Holiday Tours*, 559 F.2d at 844. Hence, a stay will not be granted in a subpoena enforcement action simply because a novel legal issue is presented. *See FEC v. Comm'n to Elect Lyndon LaRouche*, 613 F.2d 849, 853 (D.C. Cir. 1979).

definition controls." *Wolverine Power Co. v. FERC*, 963 F.2d 446, 451 (D.C. Cir. 1992). Moreover, the structure, purpose and legislative history of the DMCA fully support the conclusion that the § 512(h) subpoena authority extends to all service providers, including those (like Verizon) who fall within subsection (a)'s conduit functions. The statutory construction issue Verizon presents may be important and even novel, but that does not necessarily mean it is close or that Verizon is likely to succeed on the merits of its appeal.

Verizon contends that the Court's construction of the DMCA renders the "take down" notification within § 512(c)(3)(A)(ii) meaningless, because "material" can only be "removed" by a service provider if it is physically stored on the provider's network or system. Under subsection (a), the copyrighted material is stored on the user's own computer, and therefore a service provider cannot remove that material. Verizon therefore argues that the § 512(h) subpoena authority can only apply to subsection (c) service providers because they store such materials on their systems. However, § 512(h) requires a copyright owner to provide the clerk with a "copy of the notification *described* in subsection (c)(3)(A)." § 512(h)(2)(A) (emphasis added). It does not require a service provider to actually "take down," or disable access to, the material alleged to be infringing. Verizon confuses the obligation of the copyright owner simply to provide a "copy" of the notification "described" in subsection (c)(3)(A) with a duty actually to "take down" the material--a duty not found in or required by subsection (h). Moreover, even if one accepted Verizon's interpretation of the statute, a service provider within subsection (a) still could satisfy subsection (c)(3)(A)(iii)'s requirement to identify the material that is to be removed or to which access is to be disabled. Again, this is only an obligation to identify the alleged infringing material, not a requirement to remove or disable access to it. Finally, even if there were such a

requirement, a service provider can "disable access" to the material by terminating the subscriber's account.

An additional statutory argument raised by Verizon to justify a stay rests on § 512(n), which provides:

> Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

17 U.S.C. § 512(n). Verizon argues that the scope of the subpoena authority should be determined in light of the service provider's *function*, rather than in accordance with the definition of "service provider" in subsection (k)(1), as this Court concluded. This argument was not initially raised in the first subpoena action, but only in Verizon's stay motion--and for good reason. Subsection (n) explicitly applies only to whether a service provider qualifies for the "limitation on liability" in subsections (a) through (d), and makes no reference whatsoever to construction of the subpoena authority under subsection (h). Thus, subsection (n) cannot be read to somehow narrow the broad definition of "service provider" set out in subsection (k).[26] That

---

[26] As the Court explained in its prior decision, there is no doubt that subsection (k)'s broad definition of "service provider" applies to subsection (a) conduit functions such as providing Internet connectivity or e-mail. *See* 240 F.3d at 31. The legislative history of the DMCA makes this explicit, noting that the definition of "service provider" under subsection (k) includes "services such as providing Internet access, e-mail, chat room and web page hosting services" -- the very services within subsection (a)'s

definition is governing here, and nothing in subsection (n) is inconsistent with that conclusion.

Nor is there a substantial likelihood that Verizon will prevail on the merits of its Article III challenge to § 512(h). To be sure, the clerk of the court is not commonly called upon to issue a subpoena in the absence of a pending case or controversy. But given that the clerk only, not a federal judge, is actually involved in the issuance of a § 512(h) subpoena, and that, in any event, there is ample precedent for judicial compulsion of evidence in the absence of a pending federal court case or controversy, it is clear that the procedure authorized by § 512(h) is constitutionally permissible. Verizon thus has no more than a marginal likelihood of success on its Article III challenge.

Verizon is even less likely to prevail on its First Amendment claim. Section 512(h) does not purport to regulate speech or expression; rather, it is a tool to aid copyright owners in identifying infringers and combating Internet piracy. The subpoena provision contains a number of substantial procedural requirements aimed at preventing abuse, fraud, and mistakes, without chilling expressive or associational rights. Moreover, Verizon's overbreadth challenge fails on several grounds, and the constitutional avoidance doctrine is inapposite because a grave constitutional problem is not presented and because Verizon's suggested "saving" construction of § 512(h) is not plausible and, in any event, would only reduce, not eliminate, the alleged constitutional infirmity.

In short, there is little chance that Verizon will succeed on the merits of its statutory and constitutional claims on appeal, and surely not a "probability" or "substantial

---

conduit functions. *See* S. Rep. No. 105-190, at 54; *see also* H.R. Rep. No. 105-551(II), at 64 (1998).

likelihood" of such success. "[A] court, when confronted with a case in which the other three [stay] factors strongly favor interim relief may exercise its discretion to grant a stay if the movant has made a substantial case on the merits." *Holiday Tours*, 559 F.2d at 843. In that setting, "it will ordinarily be enough that the plaintiff has raised questions going to the merits so serious, substantial, and difficult and doubtful, as to make them a fair ground for litigation and thus for more deliberative investigation." *Id.* at 844. As explained below, however, here the balance of harms does not favor a stay, and thus it remains "particularly important for the movant to demonstrate a substantial likelihood of success on the merits." *Dodd v. Fleming*, 223 F. Supp. 2d 15, 20 (D.D.C. 2002). Verizon has not done so -- the statutory and constitutional claims it asserts are ultimately not difficult, and there is accordingly no need for further "deliberative investigation" on them. Verizon's inability to establish a likelihood of success on the merits therefore fatally undermines its stay request.

C. Balance of Harms

Both Verizon and RIAA claim forcefully that they will be irreparably injured by an adverse stay ruling from the Court. Verizon claims the denial of a stay may moot its appeal and injure its business interests, while RIAA argues that, if a stay is granted, extensive copyright infringement would continue indefinitely. RIAA also fears that other service providers may refuse to comply with DMCA subpoenas until the Court of Appeals rules, thereby delaying RIAA's investigation of copyright infringement on the Internet.

1. Injury to Verizon

To begin with, it is difficult to appreciate Verizon's claims of harm to its interests, given that Verizon has stressed throughout this litigation that RIAA could readily

obtain the identity of the alleged infringers through a John Doe action. *See* Verizon Opp. to Mot. to Enforce, No. 02-MS-0323 (Aug. 30, 2002), at 5, 24-25; *see generally First Subpoena Decision*, 240 F. Supp. 2d at 39-41. In fact, Verizon has indicated that it will cooperate with a subpoena served under a John Doe complaint, and disclose the identity of an alleged infringer. *Id.* at 24-25; Verizon Mot. for Stay, No. 02-MS-0323 (Jan. 30, 2002), at 14. If that is the case, and it is only a question of the process for disclosure of such information, then one cannot easily fathom how Verizon would truly suffer serious, irreparable harm warranting a stay.

Verizon maintains that it will be irreparably harmed by disclosure of a user's identity because that will adversely affect the goodwill Verizon has developed with its subscribers and may scare off future business. "The key word in this consideration is *irreparable*. Mere injuries, however substantial, in terms of money, time and energy necessarily expended in the absence of a stay are not enough." *Wisconsin Gas Co. v. Fed. Energy Reg. Comm'n*, 758 F.2d 669, 674 (D.C. Cir. 1985)(emphasis in original; citation omitted). Impact on business and profits "may constitute irreparable harm only where the loss threatens the very existence of the movant's business." *Id.; see also Holiday Tours*, 559 F.2d at 843 n.2. Verizon makes no showing that compliance with this one subpoena, or even with a series of subpoenas for subscribers' identities, pending appellate proceedings would threaten the very existence of its business.

In the end, then, it is difficult to discern any irreparable injury to Verizon from having to disclose, under court order, the identities of a few of its subscribers. Any harm to its goodwill is speculative and negligible. Weighing the stay factors on a sliding scale tips heavily against granting

Verizon's request for a stay where it can show only the slightest threat of irreparable injury. "Despite this flexibility, we require the moving party to demonstrate at least 'some injury,' since 'the basis for injunctive relief in the federal courts has always been irreparable harm.'" *CityFed Fin. Corp.*, 58 F.3d at 747 (quoting *Population Inst. v. McPherson*, 797 F.2d 1062, 1078 (D.C. Cir. 1986), and *Sampson v. Murray*, 415 U.S. 61, 88, 94 S. Ct. 937, 39 L. Ed. 2d 166 (1974)). Indeed, because the movant "ha[s] made no showing of irreparable injury here, that alone is sufficient for us to conclude that the district court did not abuse its discretion by rejecting [movant's] request." *CityFed. Fin. Corp.*, 58 F.3d at 747; *see also Dodd v. Fleming*, 223 F. Supp. 2d at 20 ("if a party makes no showing of irreparable injury, the court may deny the motion for injunctive relief without considering the other factors"). Without irreparable injury, Verizon simply cannot justify a stay.

2. Mootness

Verizon also contends that it will be irreparably harmed absent a stay because the revelation of its subscriber's identity would moot the appeal and deprive Verizon of its statutory right to further judicial review. *See Center for Int'l Envtl. Law v. Office of U.S. Trade Rep.*, 240 F. Supp. 2d 21, 22-23 (D.D.C. 2003) ("defendants have made a strong showing of irreparable harm because disclosure of the documents in question will render any appeal moot"); *Center for Nat'l Security Studies v. United States Dep't of Justice*, 217 F. Supp. 2d 58, 58 (D.D.C. 2002) (granting stay of disclosure order in FOIA case where compliance with order "would effectively moot any appeal"). RIAA counters that effective relief could still be granted and that the case falls within the "capable of repetition yet evading review" exception to mootness. RIAA has stated, moreover, that it will not argue mootness on

appeal. Hearing Tr., Mot. to Stay, 02-MS-0323 (Feb. 13, 2003), at 44.[27]

These subpoenas seem to fall within an exception to mootness. The Supreme Court has found "that jurisdiction is not necessarily defeated simply because the order attacked has expired, if the underlying dispute between the parties is one 'capable of repetition, yet evading review.'" *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 546, 96 S. Ct. 2791, 49 L. Ed. 2d 683 (1976) (quoting *Southern Pacific Terminal Co. v. ICC*, 219 U.S. 498, 515, 31 S. Ct. 279, 55 L. Ed. 310 (1911)). In this two-part calculus, a dispute is capable of repetition if "there [is] a reasonable expectation that the same complaining party would be subjected to the same action again," and evades review if "the challenged action was in its duration too short to be fully litigated prior to its cessation or expiration." *Weinstein v. Bradford*, 423 U.S. 147, 149, 96 S. Ct. 347, 46 L. Ed. 2d 350 (1975) (*per curiam*).

Under the capable of repetition prong, a party must show a reasonable expectation "that the same parties will engage in litigation over the same issue in the future." *Pharmachemie B.V. v. Barr Laboratories*, 276 F.3d 627, 633 (D.C. Cir. 2002) (citing *Norman v. Reed*, 502 U.S. 279, 288, 112 S. Ct. 698, 116 L. Ed. 2d 711 (1992)). Given the extent of copyright piracy occurring over the Internet today, and given that Verizon has 1.7 million customers, it is certainly likely that RIAA, which represents the vast majority of copyright owners of music, will serve more subpoenas, and attempt to enforce them, against Verizon in the future. In fact, since RIAA served these two subpoenas on Verizon, it has filed four others on Verizon seeking the identity of alleged

---

[27] Notwithstanding RIAA's commitment, the Court recognizes that mootness goes to the jurisdiction of the Court of Appeals and hence must be considered even if not asserted by the parties.

infringers. *See* Civil Action Nos. 03-MS-0071, 03-MS-0079, 03-MS-0088, and 03-MS-0089 (D.D.C. 2003).[28] There is plainly "a reasonable expectation" that Verizon "would be subjected to the same action again." *LaRouche v. Fowler*, 152 F.3d 974, 978 (D.C. Cir. 1998).

Under the "evading review" prong of the mootness exception, the question is whether "the challenged activity is *by its very nature short in duration*, so that it could not, or probably would not, be able to be adjudicated while fully live." *Id.* at 978 (emphasis in original). In the absence of a stay, RIAA's subpoenas probably would not be able to be adjudicated while fully "live," because user identities would be disclosed, satisfying the subpoena. This inquiry addresses the particular activity's temporal duration, that is, "[h]ow quickly must an activity begin and end to evade judicial review," and "evading review means evading Supreme Court review." *Campbell v. Clinton*, 203 F.3d 19, 33 (D.C. Cir. 2000) (Tatel, J., concurring). The context here -- copyright infringement over the Internet -- is inherently one that likely evades review. Section 512(h) expressly and repeatedly (in eight separate references) mandates that the subpoena process occur "expeditiously," for it is critical to curtail infringement as quickly as possible, given "the ease with which digital works can be copied and distributed worldwide virtually instantaneously." S. Rep. No. 105-190, at 8. The very nature of the speed, and worldwide scope, of copyright piracy over the Internet means that these subpoena issues could not be adjudicated while fully "live"

---

[28] Verizon's counsel has conceded that this litigation is capable of repetition. Hearing Tr., Mot. to Stay, 02-0323 (Feb. 3, 2003), at 37. Indeed, the potentially large number of these subpoenas was one of the parade of horribles Verizon has cited to illustrate the burden Internet service providers face under RIAA's construction of the DMCA. *See* Opp. to Motion to Enforce at pp. 11-13.

(unless stays were routinely entered).[29] If subpoenas could not be enforced pending the sometimes glacial pace of full appellate review, there would be little point in seeking enforcement in the first place -- it would simply take too long to protect copyrights.

3. Harm to RIAA

The harm to RIAA, and the copyright owners it represents, from a stay is comparatively more substantial than any harm to Verizon absent a stay. The extent of copyright infringement and piracy of music recordings over the Internet has skyrocketed, resulting in enormous losses for the industry. Most importantly, if the Court entered a stay, the apparent infringement of numerous copyrighted works made available over the Internet for universal downloading could continue unabated. Unauthorized use of a copyrighted work has long been presumed to constitute irreparable harm.[30] The value of these copyrighted works could plummet further, as they are made available (at the push of a button) for the taking. Given the extensive losses to Internet piracy, the relative harm to RIAA and copyright

---

[29] *See, e.g., Jefferson v. Abrams*, 747 F.2d 94, 96 (2d Cir. 1984) (in challenge to procedures for nominating candidates for special election to Congress, court reasoned that "the very speed with which such elections must be conducted makes the problem of constitutional defects in nomination procedures peculiarly one 'capable of repetition, yet evading review' ") (citing *Montano v. Lefkowitz*, 575 F.2d 378, 382 (2d Cir. 1978)).

[30] *See Health Ins. Ass'n of Am. v. Novelli*, 211 F. Supp. 2d 23, 28 (D.D.C. 2002) ("In copyright infringement cases, a copyright holder may be presumed to suffer irreparable harm as a matter of law when his right to the exclusive use of copyrighted material is invaded."); *Taylor Corp. v. Four Seasons Greetings*, 315 F.3d 1039, 1041-42 (8th Cir. 2003) (for purposes of injunctive relief "[i]n copyright-infringement cases, the general rule is that a showing of a prima facie case raises a presumption of irreparable harm"); *ABKCO Music, Inc. v. Stellar Records, Inc.*, 96 F.3d 60, 66 (2d Cir. 1996) (same).

owners is significant and more than counter-balances Verizon's claimed harm. *See Delaware River Port Auth. v. Transamerican Trailer Transp., Inc.*, 501 F.2d 917, 924 (D.C. Cir. 1974) ("Relief saving one claimant from irreparable injury, at the expense of similar harm caused another, might not qualify as the equitable judgment that a stay represents.") (citing *Virginia Petroleum Jobbers Ass'n v. Federal Power Comm'n*, 259 F.2d 921, 925 (D.C. Cir. 1958)).[31]

If a stay is entered, it is foreseeable that other service providers presented with subpoenas under the DMCA will seek a stay of enforcement pending appellate resolution of this "test" case.[32] Meanwhile, copyrighted works would remain open to infringement over the Internet.[33] In that setting, a stay could, effectively, serve as an injunction against any use of DMCA subpoena authority until a Court of Appeals decision, a scenario inconsistent with this Court's assessment of Congress's intent. "Every day [the stay]

---

[31] Verizon's assertion that RIAA and copyright owners will not be harmed because there is a three-year statute of limitations for prosecuting copyright infringement ignores the fact that monetary damages or the recovery of royalties are not realistic remedies here. It is highly unlikely that the two individuals alleged to be infringing the copyrights of more than 600 and 800 songs respectively are in a position to pay royalties and statutory damages--at $150,000 per violation--should RIAA pursue an infringement action. Moreover, the availability of money damages will not generally overcome irreparable injury resulting from copyright infringement. *See Cadence Design Systems v. Avant! Corp.*, 125 F.3d 824, 827 (9th Cir. 1997) ("a defendant cannot, by asserting the adequacy of money damages, rebut the presumption of irreparable harm that flows from a showing of likelihood of success on the merits of a copyright infringement claim").

[32] It appears that Earthlink, another service provider, may refuse to comply with DMCA subpoenas until the Court of Appeals rules. *See* RIAA Opp. to Verizon Mot. to Stay, Ex. A, ¶ ¶ 4-10 (Whitehead Decl.).

[33] Although Verizon has notified both of the alleged infringers, only one has agreed to stop, in the future, making works available over the Internet pending complete resolution of the subpoenas.

remains in force the clearly expressed intent of Congress is being frustrated." *Heckler v. Turner*, 468 U.S. 1305, 1309, 105 S. Ct. 2, 82 L. Ed. 2d 891 (1984) (Rehnquist, J., in chambers). Even though an issue of first impression may be presented here, there is negligible harm to Verizon absent a stay, particularly in contrast to the ongoing harm facing RIAA and copyright owners (by way of unabated piracy).

4. The Public Interest

Finally, the public interest will best be served by denying Verizon's request for a stay. Under the public interest prong, the views of "Congress, the elected representatives of the entire nation," are "another sense by which public interest should be gauged." *Cuomo*, 772 F.2d at 978. "[A] court sitting in equity cannot 'ignore the judgment of Congress, deliberately expressed in legislation.'" *United States v. Oakland Cannabis Buyer's Co-op.*, 532 U.S. 483, 497-98, 121 S. Ct. 1711, 149 L. Ed. 2d 722 (2001) (quoting *Virginia R. Co. v. Railway Employees*, 300 U.S. 515, 551, 57 S. Ct. 592, 81 L. Ed. 789 (1937)).[34]

It would not be in the public interest to alter the trade-offs Congress carefully crafted in the DMCA. As this Court has stated, "in exchange for complying with subpoenas under subsection (h), service providers receive liability protection from any copyright infringement . . . Hence, any additional burden [on service providers] is offset by that [liability] protection, which, of course, is exactly the contemplation reflected in the structure of the DMCA." *First*

---

[34] Indeed, in the context of a stay, "[t]he presumption of constitutionality which attaches to every Act of Congress is not merely a factor to be considered in evaluating success on the merits, but an equity to be considered ... in balancing the hardships." *Walters v. Nat'l Ass'n of Radiation Survivors*, 468 U.S. 1323, 1324, 105 S. Ct. 11, 82 L. Ed. 2d 908 (1984) (Rehnquist, J., in chambers).

Subpoena Decision, 240 F. Supp. 2d. at 34 n. 6.[35] The legislative history of the DMCA reflects the congressional balancing of the interests of service providers, copyright owners, and Internet users: "the Committee believes it has appropriately balanced the interests of content owners, on-line and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the Internet." H.R. Rep. No. 105-551(II), at 21. It would not serve the public interest for Verizon to continue to receive the benefits of the legislation--liability protection -- without the concomitant obligations of disclosing the identity of an alleged infringer.

> A district court cannot, for example, override Congress' policy choice, articulated in a statute . . . Once Congress, exercising its delegated powers, has decided the order of priorities in a given area, it is . . . for the courts to enforce them when enforcement is sought.' *Courts of equity cannot, in their decision, reject the balance that Congress has struck in a statute.*

Oakland Cannabis Buyers' Co-op., 532 U.S. at 497, 121 S. Ct. 1711 (emphasis added) (quoting *Tennessee Valley Auth. v. Hill*, 437 U.S. 153, 194, 98 S. Ct. 2279, 57 L. Ed. 2d 117 (1978)).[36]

---

[35] Other courts have recognized the trade-offs embodied in the DMCA, giving service providers copyright liability protection in exchange for assisting copyright owners to identify infringers. *See ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001); *United States v. Elcom Ltd.*, 203 F. Supp. 2d at 1124.

[36] The public interest is also advanced by the considerable deference courts have long afforded Congress in regard to the scope of copyright law, particularly when it comes to new technologies. *See Eldred*, 123 S. Ct. at 772 ("[w]e defer substantially to Congress"); *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 431, 104 S. Ct. 774, 78 L. Ed. 2d 574 (1984)

In fact, it is well-established that "the public interest is in the interest in upholding copyright protections." *Autoskill, Inc. v. Nat'l Educ. Support Sys., Inc.*, 994 F.2d 1476, 1499 (10th Cir. 1993); *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1255 (3rd Cir. 1983) ("It is virtually axiomatic that the public interest can only be served by upholding copyright protections."); *Control Data Sys. v. Infoware, Inc.*, 903 F. Supp. 1316, 1326 (D. Minn. 1995) ("the public interest is furthered by enforcing copyright laws and preventing the infringement of copyrighted materials"). Of course, copyrights serve as important incentives encouraging creativity and protecting free speech, which furthers the public interest. "By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." *Eldred*, 123 S. Ct. at 788. In short, the Court concludes that the public interest is best served by respecting the balance struck by Congress through the DMCA, and in upholding statutory copyright protections which encourage the dissemination of ideas. That conclusion warrants not only a rejection of Verizon's claims on the merits, but also rejection of the stay request based on an assessment of the public interest.

CONCLUSION

Verizon's motion to quash RIAA's February 4, 2003 subpoena is denied. The Court finds that § 512 of the

---

("Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials."). In other words, courts "are not at liberty to second-guess congressional determinations and policy judgments" regarding copyright issues, and "it is generally for Congress, not the courts, to decide how best to pursue the Copyright Clause's objectives." *Eldred*, 123 S. Ct. at 782-83. "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably complicated by such new technology." *Sony*, 464 U.S. at 431, 104 S. Ct. 774.

DMCA, as construed by this Court in its *First Subpoena Decision*, does not violate the "case or controversy" requirement of Article III of the Constitution, and does not abridge the First Amendment rights of Internet users. Because Verizon cannot demonstrate that it has a substantial likelihood of prevailing on the merits of its statutory or constitutional claims, and has not shown that it will be irreparably harmed if a stay pending appeal is not granted, Verizon has not met its heavy burden "to justify the court's exercise of such an extraordinary remedy." *Cuomo*, 772 F.2d at 978. Verizon's request for a stay pending appeal is therefore denied.

Separate orders in this case and in Civil Action No. 02-MS-0323 (JDB) have been issued on this date.

Appendix D

United States Court of Appeals
For the District of Columbia Circuit

No. 03-7015 **September Term, 2003**
02ms00323
02ms00040

Recording Industry Association of American, Inc.
Appellee
v.
Verizon Internet Services, Inc.
Appellant

Consolidated with 03-7053 Filed on Feb. 24, 2004

BEFORE: Ginsburg, Chief Judge, Roberts, Circuit Judge, and Williams, Senior Circuit Judge

ORDER

Upon consideration of appellee's petition for rehearing filed February 2, 2004, it is

ORDERED that the petition be denied.

Per Curiam

FOR THE COURT:
Mark J. Langer, Clerk

/s/

BY: Michael C., McGrial
Deputy Clerk

Appendix E

United States Court of Appeals
For the District of Columbia Circuit

No. 03-7015 **September Term, 2003**
02ms00323
02ms00040

Recording Industry Association of American, Inc.
Appellee
v.
Verizon Internet Services, Inc.
Appellant

Consolidated with 03-7053 Filed Feb. 24, 2004

BEFORE: Ginsburg, Chief Judge, Edwards, Sentelle, Henderson,* Randolph, Rogers, Tatel, Garland, and Roberts, Circuit Judges, and Williams, Senior Circuit Judge

ORDER

Upon consideration of appellee's petition for rehearing en banc, and the absence of a request by any member of the court for a vote, it is

ORDERED that the petition be denied.

Per Curiam

FOR THE COURT:
Mark J. Langer, Clerk
/s/
BY: Michael C., McGrial
Deputy Clerk

* Circuit Judge Henderson did not participate in this matter.

Appendix F

17 U.S.C. § 512

§ 512. Limitations on liability relating to material online

(a) **Transitory digital network communications.** A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for

the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System caching.

(1) Limitation on liability. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

(2) Conditions. The conditions referred to in paragraph (1) are that

(A) the material described in paragraph (1) is transmitted to the subsequent users described in

paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the

originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information residing on systems or networks at direction of users.

(1) In general. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider

(A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) **Designated agent.** The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) **Elements of notification.**

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online

site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B) (i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) **Information location tools.** A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on liability of nonprofit educational institutions.

(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) **Misrepresentations.** Any person who knowingly materially misrepresents under this section

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys" fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it

(g) Replacement of removed or disabled material and limitation on other liability.

(1) No liability for taking down generally. Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception. Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first

receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) **Contents of counter notification.**--To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided

notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability. A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena to identify infringer.

(1) Request. A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request. The request may be made by filing with the clerk

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena. The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) **Basis for granting subpoena.** If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) **Actions of service provider receiving subpoena.**

Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) **Rules applicable to subpoena.** Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) **Conditions for eligibility.**

(1) **Accommodation of technology.** The limitations on liability established by this section shall apply to a service provider only if the service provider

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy

that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) **Definition.**As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) **Injunctions.** The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) **Scope of relief.**

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material

or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to

a specific, identified, online location outside the United States.

(2) **Considerations.** The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) **Notice and ex parte orders.** Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions.

(1) Service provider.

(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary relief. As used in this section, the term "monetary relief" means damages, costs, attorneys" fees, and any other form of monetary payment.

(l) Other defenses not affected. The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of privacy. Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) **Construction.** Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

Appendix G

[Dept. of Justice Seal]

U.S. Department of Justice
Civil Division, Appellate Staff
601 "D" Street, N.W., Rm: 9550
Washington, D.C. 20530

SRMcIntosh
233279-2108

Tel: (202 514-4052
Fax: (202) 514-7964

September 22, 2003

Mr. Mark J. Langer
Clerk, United States Court of Appeals
for the District of Columbia Circuit
United States Courthouse
Room 5423
Third & Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Recording Industry Association of America v.
Verizon Internet Services, Inc.
Nos. 03-7015 & 03-7053

Dear Mr. Langer:

Oral argument in this case was heard on September 17 before Judges Ginsburg, Williams, and Roberts. During the argument, Judge Roberts asked counsel for the United States about the government's views regarding the meaning of 17 U.S.C. § 512(h). Counsel informed Judge Roberts that the Copyright Office agrees with the district court's interpretation of Section 512(h).

The views of the Copyright Office regarding the proper construction of Section 512(h) were presented publicly by the Register of Copyrights, Marybeth Peters, in testimony before the Senate Committee on the Judiciary on September 9, 2003. If the members of the panel are interested in those views, Ms. Peters's statement to the Judiciary Committee is available at http://www.copyright.gov/docs/regstat090903.html.

I would appreciate if it you would bring this information to the attention of the Court. Thank you for your assistance.

Sincerely,

/s/
Scott R. McIntosh
Attorney, Appellate Staff
Civil Division

[Service list omitted]

Appendix H

Statement of Marybeth Peters
The Register of Copyrights
before the
Committee on the Judiciary

United States Senate
108th Congress, 1st Session

September 9, 2003

Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks

Mr. Chairman, Senator Leahy, Members of the Committee, good afternoon. It is always a pleasure to appear before this Committee and I thank you for inviting me to present the views of the Copyright Office today at this very timely hearing. As you were among the leaders in drafting and enacting the Digital Millennium Copyright Act ("DMCA"), I know that these issues are important to you, as they are to me.

I. Background

In 1999, a young man named Shawn Fanning developed a use of the Internet that allowed people to identify and copy music files from other people's computers. As you know, this model popularized peer-to-peer technology and a company called Napster tried to turn it into a profit-making business. Napster became phenomenally popular in a remarkably short period of time, boasting millions of registered users the very next year. But it quickly became clear that Napster was being used extensively (by millions of users) for the purpose of copying and distributing an

unprecedented number of copyrighted works, primarily sound recordings of musical works.

That was the scene when you held a hearing on July 11, 2000, Mr. Chairman, entitled "Music on the Internet: Is There an Upside to Downloading?" At that hearing, Mr. Hank Barry, then the CEO of Napster, stated "It is my firm belief that the consumers who use Napster are *not* committing copyright violations."[1] We did not agree with that assessment,[2] and we were heartened when the Ninth Circuit found that "Napster users infringe at least two of the copyright holders' exclusive rights: the rights of reproduction...and distribution."[3] Napster was unable to find a way to continue operations and faded away.

The void left by Napster's departure was filled by other businesses utilizing peer-to-peer technology, such as Aimster, Grokster, and Kazaa. While some of these applications can be differentiated from Napster in terms of their internal technical operation, they still follow the same basic peer-to-peer model as Napster and it is apparent that an overwhelming number of their customers are using it for the same purpose as they and others had used Napster - copying and distributing copyrighted works. By now it is well-settled that those users are infringing copyright. Notwithstanding that, there are still some who contend that such uses are not infringing. [4]

Mr. Chairman, make no mistake. The law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works without permission is infringement and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue has agreed that this activity is infringement.[5] It can also be a crime and the perpetrators of such a crime are subject to fines and jail time.

Some have tried to rationalize or justify their illegal behavior by attacking the victim with allegations of inflated profits or unfair dealings with recording artists on the part of the recording industry. These diversionary tactics do not alter the fundamental fact that they are trying to defend illegal activity that takes place on peer-to-peer networks. For those who do not have sympathy for the recording industry, there are other victims as well. Since Napster, subsequent versions of peer-to-peer networks permit infringement of the works of other copyright owners, large and small, from motion picture studios to independent photographers and needlepoint designers. With broadband connections becoming more and more widespread, it is increasingly more common that the larger files containing full-length motion pictures are copied back and forth.(6) This problem is not shrinking; it is not static; it is growing.

There are some who argue that copyright infringement on peer-to-peer systems is not truly harmful to copyright owners and may even help them generate new interest in their products. The law leaves that judgment to the copyright owner and it ought not be usurped by self-interested third parties who desire to use the copyright owner's work.

II. Copyright Liability of Peer-to-Peer Proprietors

Copyright law has long recognized that those who aid and abet copyright infringement are no less culpable than the direct infringers themselves.(7) There are two types of this secondary liability. Contributory infringement occurs when "[o]ne who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another."(8) For purposes of this test, knowledge can be either actual or constructive - that is, having reason to know.(9) Vicarious liability occurs when one "has the right

and ability to supervise the infringing activity and also has a direct financial interest in such activities."[10]

Both of these concepts were brought to bear in the case against Napster. The Ninth Circuit agreed with the District Court that Napster had actual knowledge of the infringements it was facilitating from, for example, notices from aggrieved copyright owners.[11] There was little question but that Napster provided a material contribution in the form of "the site and facilities" for infringement.[12] Thus, Napster was determined to be a contributory infringer.

The Ninth Circuit also considered whether Napster was vicariously liable. It had no difficulty agreeing with the District Court that the infringing material on its network was a "draw" for customers, thus providing a direct financial benefit from the infringing activity.[13] The Ninth Circuit also agreed with the District Court that Napster had the ability to police its system, and thus that it had the right and ability to supervise its users' conduct.[14] Accordingly, Napster was found to be vicariously liable as well.

Thus it was that many felt reassured that the Ninth Circuit had confirmed that copyright law provides an effective and efficient way in which to address the massive infringements that can and do occur on peer-to-peer networks. Unfortunately, the *Napster* decision was not the final word on the matter.

Earlier this year, the Central District of California surprised many when it held that Grokster and Kazaa are not liable as secondary copyright infringers.[15] This decision departed from long-established precedent. For example, the court held that in order to establish contributory liability, it must be shown that "a defendant has actual - not merely constructive - knowledge of the infringement at a time

during which the defendant materially contributes to that infringement."(16) Were such a standard to be adopted it would eviscerate the doctrine of contributory infringement as it would be almost impossible to meet. It would encourage the kind of sophistry we have seen from the proprietors of some peer-to-peer applications: a denial of knowledge of infringements by their customers in the face of clear and uncontested evidence that such infringement is occurring on a mind-boggling scale. Mr. Chairman, these are people whose business plan is dependent upon massive copyright infringement and any application of the law that allows them to escape liability for lack of knowledge of those same infringements is inherently flawed.

Not only was the *Kazaa* decision wrong on the law, it has serious policy consequences as well. The historical doctrines of secondary liability have served copyright owners, courts, and the public well - they provide copyright owners with the ability to obtain relief against the root cause of a series of infringements without costly, inefficient, and burdensome suits against numerous individuals.(17) Without a viable doctrine of contributory liability, this option is severely curtailed and may present the copyright owner with the unenviable choice of either accepting unremedied infringements or filing numerous suits against the individual direct infringers.

If today's hearing leaves the Committee with the impression that the law is in flux with regard to the liability of proprietors of peer-to-peer technology, that is because it is. On one side is the *Napster* decision of the Ninth Circuit and the *Aimster* decision of the Seventh Circuit, both finding liability, albeit through different paths of analysis. On the other side is the *Kazaa* decision of the Central District of California, finding no liability for Kazaa and Grokster. Hanging over all of these cases is the Supreme Court's

decision in *Sony*. It is perhaps a commentary on that opinion that almost twenty years later, we still have such uncertainty that three courts seem to interpret and apply it in three different ways. I believe that the correct application of the doctrines of secondary liability and the *Sony* case should produce findings of liability for the proprietors of Kazaa and Grokster as well as Napster and Aimster. If the case law evolves so as to compel the opposite result, I believe that *Sony* should be revisited either by the Supreme Court or by Congress.

III. Suits Against Individuals

Unless and until the *Kazaa* decision is overruled, copyright owners are faced with the unenviable choice to which I referred earlier. They can either resign themselves to unremedied infringements on a previously unimaginable scale, or they can file infringement actions against individual peer-to-peer users. The recording industry has chosen the latter route.

While copyright owners have expressed regret that they have felt compelled to take this step, they need offer no apologies. As I have already said, people who use peer-to-peer technology for the unauthorized reproduction or distribution of copyrighted works are breaking the law. Surprisingly, many people do not appear to realize this. I have long advocated more public education about copyright. In a perfect world, this could be done in classrooms and with billboards. But ours is not a perfect world, and public education can also be accomplished through enforcement of copyright.

The threats of litigation and even the publicity about the subpoenas obtained by the RIAA have made clear to everyone that the so-called "file-sharing" of copyrighted works is not an innocent activity without legal

consequences. As a result, it is becoming more and more difficult for people engaged in such activity to claim that they did not know what they were doing is against the law. Of course, for some users of peer-to-peer technology, even knowledge that what they are doing is illegal will not be a sufficient disincentive to engage in such conduct. But whether or not these infringers know or care that it is against the law, the knowledge that such conduct may lead to expensive and burdensome litigation and a potentially large judgment should have a healthy deterrent effect. While we would like to think that everyone obeys the law simply because it is the law and out of a sense of obligation, we also know that laws without penalties may be widely ignored. For many people, the best form of education about copyright in the internet world is the threat of litigation. In short, if you break the law, you should be prepared to accept the consequences. Copyright owners have every right to enforce their rights in court, whether they are taking action against providers of peer-to-peer services designed to profit from copyright infringement or against the persons engaging in individual acts of infringement using such services.

IV. Statutory History and Interpretation of Subsection 512(h)

It is common sense that in order to be able to take action against the users of peer-to-peer networks, the copyright owner must know who those users are.[18] Congress foresaw this need and addressed it by including in the DMCA a process by which copyright owners can learn basic identifying information about alleged infringers from their internet service providers ("ISPs").[19]

The DMCA began as an effort to implement the 1996 WIPO Internet treaties.[20] Neither those treaties nor any other international instrument directly address the potential secondary liability of ISPs. However, as the treaty

implementing legislation moved forward in Congress, representatives of ISPs demanded that the legislation also limit their liability under such circumstances.(21) Congress heeded this call and provided the ISPs with a huge benefit - virtually no liability for qualifying ISPs. This was balanced by a carefully developed set of obligations in the DMCA. Among those balancing obligations was the requirement that ISPs "expeditiously" respond to subpoenas to provide identifying information about subscribers accused of copyright infringement so that the controversy could be settled in court.

At the time the DMCA was drafted, at least one representative of ISPs assured this Committee that ISPs desired a solution whereby "service providers and content owners...work as a partnership...."(22) It was asserted by that same representative that "[l]iability for copyright infringement should fall where it belongs, on the Web site operators, on those who create an infringing work or on those who reproduce it or perform it with actual knowledge of the infringement...."(23) The ability of copyright owners to utilize subsection 512(h) is a critical part of that partnership as is copyright owners' ability to impose liability against those who infringe copyright. It is regrettable that at least one major ISP now rejects the compromise and the balance of the DMCA.

Some now claim that the subpoena power of subsection 512(h) is inapplicable to the activity described in subsection 512(a). As the United States District Court for the District of Columbia recently held, the plain language of subsection 512(h) demonstrates that this interpretation is not correct.(24) I agree with the court's analysis.

Subsection 512(h) instructs service providers to expeditiously respond to a subpoena. The definition of "service provider" in section 512(k) always includes service

providers which qualify for the safe harbor in section 512(a). The court reasoned that this demonstrates Congress' intent to apply the subpoena power to "all service providers, regardless of the functions a service provider may perform under the four categories set out in subsections (a) through (d)."[25]

It has also been argued that the subpoena power applies only to subsection 512(c) because subsection 512(h)(2)(A) requires a copyright owner to supply "a copy of a notification described in subsection (c)(3)(A)". However, as the District Court pointed out, subsection 512(h) "is written without limitation or restriction as to its application."[26] It does not require that a notice be delivered. Had Congress wished to limit the application of the subpoena power, it would have simply said so in the law. It did not.[27]

The statutory text confirms the policy of compromise behind subsection 512 -- that copyright owners and ISPs work together to remedy infringement. Limiting the subsection 512(h) subpoena provisions as some have proposed would remove an important tool that parties need to remedy infringement efficiently in the peer-to-peer context.

When it enacted the DMCA, Congress did not carve out an exception from subsection 512(h) for transitory digital network communications, the activity covered by subsection 512(a). Service providers which engage in that activity received the benefits and burdens of the same bargain that service providers engaged in the other activity covered by section 512 received. In exchange for a powerful limitation on liability, they undertook some obligations, including the obligation to identify alleged infringers when served with a subsection 512(h) subpoena. When you enacted section 512, you made the right choice. There is no reason for the courts or Congress to have second thoughts about that decision.

I understand that the majority if not all of the 512(h) subpoenas that have been sought, have been sought in the United States District Court for the District of Columbia. Apparently this has necessitated the clerk of that court assigning additional staff to handle the workload. I do not take a position as to whether it is appropriate for a copyright owner to go to a single district court for subpoenas to service providers located outside that district. However, I am sympathetic to concerns about efficiency of the courts and fairness to ISPs located elsewhere in the country. There would certainly be advantages to the filing of these subpoena requests in the districts in which the ISPs are located.

V. Constitutional Challenges to Subsection 512(h)

The United States has intervened in the Verizon-RIAA litigation to defend the constitutionality of the DMCA. The Copyright Office has assisted the Justice Department in this effort and we firmly believe that subsection 512(h) is appropriate and constitutional. Although I am not an expert on constitutional law and I am not here to represent the Department of Justice, I will briefly summarize the arguments the United States made in its brief to the District Court.

The claim that subsection 512(h) violates the case and controversy requirement of the Constitution is belied by a review of other federal laws providing similar procedures, at least one of which has a 150 year pedigree.[28] The 512(h) procedure is also similar to discovery in advance of federal litigation pursuant to Federal Rule of Procedure 27, which finds its origins in the Judiciary Act of 1789.[29] Further, the subpoena power provided in subsection 512(h) does relate to cognizable Article III controversies, namely potential copyright infringement action as well as a dispute between

the copyright owner and the ISP over access to the subscriber information.[30]

The claim that subsection 512(h) violates the First Amendment does not withstand scrutiny. Subsection 512(h) does not proscribe spoken words or expressive or communicative conduct,[31] nor is there a realistic danger that it will significantly compromise a recognized First Amendment protection.[32] Section 512(h) merely requires a service provider to identify a person who appears to be engaging in copyright infringement, a necessary step before the copyright owner can initiate legal action. That action may range from an email or letter demanding that the alleged infringer cease and desist from the unlawful conduct to the filing of a lawsuit for copyright infringement. Section 512(h) does not offend the First Amendment any more than the filing of a lawsuit for copyright infringement. In fact, it is an essential tool for a copyright owner who intends to file such a lawsuit. Moreover, indeed, section 512 imposes sanctions on those who misuse the subpoena power, which serve to provide a safeguard.[33]

Although not addressed in the Government's briefs in intervention, I think it is important to put into context the privacy claims that some now put forward. Users of peer-to-peer networks are, by definition, opening their computers up to the world. There may be an illusion of anonymity to that activity, but we have come to learn that such connections can also make available the user's social security number, credit card numbers, and other vital information. By contrast, the 512(h) subpoena process typically involves disclosure to the copyright owner of no more than the subscriber's name, email address, phone number, and perhaps street address. This hardly seems like an invasion of privacy.

VI. Conclusion

The DMCA represents a carefully crafted and balanced bargain which utilizes the incentives created by pre-existing doctrines such as secondary liability as well as enlightened self-interest to encourage all stakeholders to work cooperatively to realize the potential of the Internet while respecting legal rights. Some are now selectively challenging key components of that bargain, particularly in the context of peer-to-peer technology. Taken together, the positions of Kazaa and Grokster, along with the arguments now made by Verizon, if they prevail, will leave copyright owners with little or no remedy against the most widespread phenomena of infringement in the history of this country. We know from past experience with Napster and current experience with Kazaa and Grokster that without a judicial remedy, this infringement will not stop, regardless of the availability of lawful alternatives. It is thus incumbent upon this Committee and this Congress to see to it that if the judiciary fails to enforce the DMCA and therefore fails to provide the protection to which copyrighted works are entitled, the legislature does.

---

1. Submitted Testimony, Hank Barry, p. 7 (emphasis in original).

2. See Brief for the United States as *Amicus Curiae* at 11, n.1, 18, *A&M Records, Inc. v. Napster*, 293 F.3d 1004 (9th Cir. 2001) (Nos. 00-16401 & 00-16403).

3. *A&M Records v. Napster*, 293 F.3d 1004, 1014 (9th Cir. 2001) (hereinafter "*Napster*").

4. Los Angeles Times, "Tone Deaf to a Moral Dilemma?" (Sept. 2, 2003).

5. See *Napster* at 1014; *In re: Aimster Copyright Litigation*, 334 F.3d 643, 645 (7th Cir. 2003) (hereinafter "*Aimster*"); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1034-35 (C.D. Cal. 2003) (hereinafter "*Kazaa*").

6. See Gary Gentile, "Online Movie Service Quickens Downloads," Associated Press, September 3, 2003.

7. See *Kalem Co. v. Harper Bros.*, 222 U.S. 55, 63 (1911).

8. *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

9. *Id.*

10. *Id.*

11. *Napster* at 1020-21.

12. *Id.* at 1022 (*quoting Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996) (hereinafter "*Fonovisa*")).

13. *Id.* at 1023 (quoting *Fonovisa* at 263-64).

14. *Id.* at 1023-24.

15. *Kazaa*, 259 F. Supp. 2d 1029.

16. *Id.* at 1036.

17. See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 437, n.18 (hereinafter "*Sony*") (citing the "dance hall cases"); *Fonovisa*, 76 F.3d 259 (suit against the operator of a swap meet for infringing activity of third-party vendors).

18 The existence of section 512(h) is plain evidence that Congress did not view any existing procedures by which a suit could be filed against an unknown defendant as acceptable alternatives for copyright owners.

19. See 17 U.S.C. § 512(h).

20. See *Hearings on S. 1121 Before the Senate Judiciary Committee*, 105th Cong. 25 (statement of George Vradenburg, III) (representing "over 1,400 Internet service providers, content creators, telephone companies, among others. . .").

21. *Id.*

22. *Id.*

23. *Id.*

24. *In re: Verizon Internet Services, Inc., Subpoena Enforcement Matter*, 240 F. Supp. 2d 24, 30 (D.D.C. 2003).

25. *Id.* at 31.

26. *Id.* at 33.

27. *Id.*

28. Brief for Intervenor United States of America, p. 6, *In re: Verizon Internet Services, Inc., Subpoena Enforcement Matter*, 257 F. Supp. 2d 244 (D.D.C. 2003) (No. 03-MS-0040 (JDB)).

29. *Id.* at 10-11.

30. *Id.* at 9, 13.

31. *Id.* at 15-16.

32. *Id.* at 16-18.

33. *Id.* at 17-18.

Supreme Court, U.S.
FILED
JUN 25 2004
OFFICE OF THE CLERK

(3)

No. 03-1579

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,

Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF IN OPPOSITION

ANDREW G. MCBRIDE
KATHRYN COMERFORD TODD
BRUCE G. JOSEPH
KARYN K. ABLIN
DINEEN PASHOUKOS WASYLIK
WILEY REIN & FIELDING LLP
1776 K Street NW
Washington, D.C. 20006
(202) 719-7000

JOHN THORNE*
SARAH B. DEUTSCH
THOMAS M. DAILEY
LEONARD CHARLES SUCHYTA
VERIZON COMMUNICATIONS INC.
1515 N. Courthouse Road
Fifth Floor
Arlington, Va. 22201
(703) 351-3900

Attorneys for Respondent

* *Counsel of Record*

188140

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

COUNTER STATEMENT OF QUESTIONS PRESENTED

1. Whether the D.C. Circuit, applying well-established canons of statutory construction, correctly concluded that the text, structure, and legislative history of the novel subpoena provision of the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), all demonstrate that that provision applies only to circumstances in which potentially infringing material is stored on the Internet service provider's system or network.

2. Whether Petitioner's expansive interpretation and use of the novel subpoena provision contained in the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), is precluded by the First Amendment to the United States Constitution.

3. Whether the issuance and enforcement of binding judicial process pursuant to 17 U.S.C. § 512(h), outside the context of a "case or controversy," violates Article III of the United States Constitution and fundamental principles of the constitutionally mandated separation of powers.

PARTIES TO THE PROCEEDING

Petitioner Recording Industry Association of America, Inc. was the appellee below. Respondent Verizon Internet Services Inc. was the appellant. The United States intervened pursuant to 28 U.S.C. § 2403 solely to defend the constitutionality of the subpoena provision of the Digital Millennium Copyright Act.

RULE 29.6 DISCLOSURE

Respondent is a wholly owned subsidiary of Bell Atlantic Entertainment and Information Services Group, Inc. Bell Atlantic Entertainment and Information Services Group, Inc. is a wholly owned subsidiary of Bell Atlantic Investment Development Corporation, which is a wholly owned subsidiary of Verizon Investments Inc. Verizon Investments Inc. is a wholly owned subsidiary of Verizon Communications Inc., a publicly held corporation. Verizon Communications Inc. does not have a parent company, and no publicly held company has a ten-percent or greater interest in it.

TABLE OF CONTENTS

	Page
Counter Statement of Questions Presented	i
Parties to the Proceeding	ii
Rule 29.6 Disclosure	ii
Table of Contents	iii
Table of Cited Authorities	vi
Table of Appendices	xii
Jurisdiction	1
Constitutional and Statutory Provisions Involved	1
Summary of Reasons for Denying the Petition	2
Statement of the Case	3
A. Legal and Factual Background	3
1. The Statutory Framework and Legislative Purpose of the DMCA	3
2. The Two Subpoenas at Issue in These Proceedings	9
B. The Proceedings Below	10
1. The District Court's Decisions	10
2. The Court of Appeals' Reversal of the District Court	11

Contents

Page

Reasons for Denying the Petition 14

I. The Petition Meets None Of The Established Justifications For Intervention By This Court. 14

A. There Is No Split of Authority on the Narrow Statutory Issue Resolved by the D.C. Circuit. 14

B. No Extraordinary Circumstances Justify Review. 15

C. RIAA's Policy Arguments Regarding New Technologies and Requests To Expand Copyright Protections Are Properly Addressed to Congress, Not to this Court. 16

II. The Court Of Appeals Correctly Applied Settled Canons Of Statutory Construction. 19

A. The Text, Structure, History, and Purpose of Section 512 Compel the Result Reached by the D.C. Circuit. 19

1. The Text and Structure of Section 512 Compel the Conclusion That Section 512(h) Applies Only to Material Stored on a Service Provider's System or Network. 19

Contents

Page

2. The Legislative History and Purpose of the Statute Further Confirm That Section 512(h) Does Not Apply to the Conduit Context. 24

B. The D.C. Circuit's Reading of the Statute Avoids Serious First Amendment Concerns. 25

C. The Existence of a Substantial Alternative Ground for Affirming the Judgment Below Militates Against Granting the Petition. 27

Conclusion 30

TABLE OF CITED AUTHORITIES

Page

CASES

Bennett v. Spear,
520 U.S. 154 (1997) 28

Blount v. Rizzi,
400 U.S. 410 (1971) 26

Buckley v. Valeo,
424 U.S. 1 (1976) 30

Christensen v. Harris County,
529 U.S. 576 (2000) 25

Columbia Insurance Co. v. Seescandy.com,
185 F.R.D. 573 (N.D. Cal. 1999) 26

E. Microwave, Inc. v. Doubleday Sports,
691 F.2d 125 (2d Cir. 1982) 4

Eldred v. Ashcroft,
537 U.S. 186 (2003) 18

Estate of Joseph Leder v. Commissioner of Internal Revenue,
893 F.2d 237 (10th Cir. 1989) 21

FDA v. Brown & Williamson Tobacco Corp.,
529 U.S. 120 (2000) 21

Freedman v. Maryland,
380 U.S. 51 (1965) 26

Cited Authorities

	Page
Gordon v. United States, 117 U.S. Appx. 697 (1864)	28
Hayburn's Case, 2 U.S. (2 Dall.) 408 (1792)	28
Hoffmann-La Roche, Inc. v. Sperling, 493 U.S. 165 (1989)	1, 28
In re Subpoena to North Carolina State University, No. 1:03mc139 (M.D.N.C.)	14
In re Subpoena to University of North Carolina, No. 1:03mc138 (M.D.N.C.)	14
Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803)	1, 28
McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)	25
Muskrat v. United States, 219 U.S. 346 (1911)	28
Overseas Education Association v. FLRA, 824 F.2d 61 (D.C. Cir. 1987)	21
Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767 (1986)	26
RIAA v. Charter Communications, Inc., No. 03-3802 (8th Cir.)	14

Cited Authorities

Page

S&E Contractors, Inc. v. United States,
406 U.S. 1 (1972) 24

Sony Corp. of Am. v. Universal City Studios, Inc.,
464 U.S. 417 (1984) 13, 18

Stanley v. Georgia,
394 U.S. 557 (1969) 27

Steel Co. v. Citizens for a Better Environment,
523 U.S. 83 (1998) 1, 27

United States v. Ferreira,
54 U.S. (13 How.) 40 (1851) 28

United States v. Mead Corp.,
533 U.S. 218 (2001) 25

United States v. Morton Salt Co.,
338 U.S. 632 (1950) 1, 28, 29

United States Catholic Conference v. Abortion Rights Mobilization, Inc.,
487 U.S. 72 (1988) 1, 28, 29

United States Railroad Retirement Board v. Fritz,
449 U.S. 166 (1980) 24

Williams v. Taylor,
529 U.S. 362 (2000) 22

Yale Todd's Case, printed at 54 U.S.
(13 How.) 52 (1851) 28

Cited Authorities

Page

CONSTITUTION AND STATUTES

U.S. Const. amend. I 1

U.S. Const. art. III ..... *passim*

17 U.S.C. § 512 1

17 U.S.C. § 512(a) ..... *passim*

17 U.S.C. § 512(b) ..... *passim*

17 U.S.C. § 512(c) ..... *passim*

17 U.S.C. § 512(d) ..... *passim*

17 U.S.C. § 512(f) 6, 20, 23, 27

17 U.S.C. § 512(g) ..... *passim*

17 U.S.C. § 512(h) ..... *passim*

17 U.S.C. § 512(i) 5, 22

17 U.S.C. § 512(j) 5, 21, 22

17 U.S.C. § 512(k) 12

17 U.S.C. § 512(m) 9

17 U.S.C. § 512(n) 6

17 U.S.C. § 1201 ..... 1, 3

17 U.S.C. § 1202 ..... 1, 3

Cited Authorities

	Page
17 U.S.C. § 1203	1, 3
17 U.S.C. § 1204	1, 3
17 U.S.C. § 1205	1, 9
28 U.S.C. § 956	30
28 U.S.C. § 2403	ii

LEGISLATIVE MATERIALS

H.R. Rep. No. 105-551 (1998)	8
S. Rep. No. 105-190 (1998)	3, 6
Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary, 105th Cong. 77 (1997) (statement of Robert W. Holleyman II, President, Business Software Alliance).	25
Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Committee on the Judiciary, 108th Cong. (Sept. 9, 2003)	8

MISCELLANEOUS

Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sept. 24, 2003	17
P. Huber, *et al.*, Federal Telecommunications Law (2d ed. 1999)	4

Cited Authorities

Page

Jan 21, 2004 RIAA Press Release, *at* http://www.riaa.com/news/newsletter/012104.asp (visited June 21, 2004) 15

John Borland, *RIAA takes hundreds more 'John Does' to court*, CNET News.com (June 22, 2004), *at* http://zdnet.com.com/2102-1104_2-5243587.html? (visited June 22, 2004) 15

Inquiry Concerning the Deployment of Advanced Telecommunications Capability, 14 F.C.C.R. 2398 (1999) 8

Mar. 25, 2004 Transcript of Q&A With RIAA President Cary Sherman, *at* http://www.dailytexanonline.com/news/2004/03/25/Focus/Transcript.Of.Qa.With.Riaa.President.Cary.Sherman-641217.shtml (visited June 14, 2004) 16

http://www.alsscan.com/copyright.html 17

RIAA nearing 1,000 subpoenas against file-sharing suspects, Pioneer Press (July 18, 2003), *at* http://www.twincities.com/mld/pioneerpress/business/technology/6335275.htm?1c (visited June 21, 2004) 30

TABLE OF APPENDICES

	Page
Appendix A — Article III Of The United States Constitution	1a
Appendix B — First Amendment To The United States Constitution	3a
Appendix C — Title I Of The Digital Millennium Copyright Act Of 1998, As Codified At 17 U.S.C. §§ 1201-1205	4a
Appendix D — Title II Of The Digital Millennium Copyright Act Of 1998, As Codified At 17 U.S.C. § 512	33a

JURISDICTION

Respondent has consistently maintained that the United States District Court for the District of Columbia lacked Article III jurisdiction to issue or enforce the subpoenas at issue here because they were not issued in furtherance of the resolution of any pending case or controversy. *See, e.g., United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950); *United States Catholic Conf. v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988); *Hoffmann-La Roche, Inc. v. Sperling*, 493 U.S. 165, 172-74 (1989).

Respondent does not, however, contest the jurisdiction of the court of appeals or this Court to examine the federal questions whether these subpoenas were properly issued under the relevant statute and whether their issuance and enforcement lies outside the judicial power as defined by Article III, section 2 of the U.S. Constitution. Pet. 2a n.1, *id.* at 60a n.6; *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83 (1998). At the very least, this Court has jurisdiction to determine whether the district court had jurisdiction to conduct any subpoena enforcement proceedings, as this Court always has jurisdiction to examine its own jurisdiction and the jurisdiction of the courts below. *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This matter involves the subpoena provision of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512(h), and implicates both Title I and Title II of the Act. Title I, *id.* §§ 1201-1205, is reprinted herein at 4a-32a; Title II, *id.* § 512, is reprinted at 33a-51a. This matter also involves Article III of the U.S. Constitution, reprinted at 1a-2a, and the First Amendment, reprinted at 3a.

SUMMARY OF REASONS FOR DENYING THE PETITION

The petition for certiorari should be denied because it satisfies *none* of the criteria specified by this Court's rules or decisions for issuance of the writ. Not surprisingly, the petition fails to cite this Court's Rule 10 or any authority that supports certiorari in the circumstances of this case. A unanimous panel of the D.C. Circuit (Ginsburg, C.J., Roberts, J., and Williams, S.J.) correctly decided a discrete issue of statutory construction by careful examination of the plain language, structure, legislative history, and purpose of the statutory provision at issue. No member of that court even called for a response to RIAA's petition for rehearing and rehearing en banc.

The court of appeals also quite properly observed that the application of copyright laws to new technologies requires a careful balancing of interests that this Court repeatedly has held is for Congress, not the federal courts, to perform. The D.C. Circuit is the first appellate court in the nation to address the scope of the DMCA's novel subpoena provision and whether it applies to new peer-to-peer technology. Its statutory analysis and conclusions are fully consistent with the decisions of this Court and do not conflict with the decision of any federal or state appellate court.

Nor are there any extraordinary circumstances that would justify deviation from this Court's normal criteria for issuance of the writ. Copyright owners possess and are vigorously employing numerous legal tools to combat on-line infringement, and Petitioner's own President has publicly stated that the D.C. Circuit's decision has not impeded RIAA's enforcement efforts in the slightest. In addition, the relevant House and Senate Committees have held extensive hearings on the proper legislative response to new peer-to-peer applications, which were not contemplated by Congress when it enacted the DMCA. For these reasons, use of this Court's limited resources to review the decision below is neither necessary nor appropriate.

STATEMENT OF THE CASE

A. Legal and Factual Background

1. The Statutory Framework and Legislative Purpose of the DMCA

The DMCA amended the Copyright Act as part of Congress's first attempt to balance copyright owners' interests in enforcing their property rights against the rights of Internet service providers and the more than 100 million individual Internet users in this country. To this end, Title I of the DMCA, entitled "Copyright Protection and Management Systems" in Title 17 of the U.S. Code, is focused primarily on helping copyright owners to protect their property rights and provides them with powerful new civil and criminal remedies to prevent the circumvention of technological "self help" measures. 17 U.S.C. §§ 1201-1204. These include protection of encryption and other access control technologies and severe penalties for falsifying, removing, or altering digital "watermarks" or other copyright management information.

Title II of the DMCA, entitled "Limitations on liability relating to material online" in Title 17, codified a set of limited immunities for Internet service providers and was intended to "ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand." S. Rep. No. 105-190, at 2 (1998). These immunities, and the duties that service providers must undertake to claim them, turn entirely on the particular function the provider is performing in relation to the creation, storage, and dissemination of Internet content or material, functions that are separately described in subsections (a) through (d) of Title II. 17 U.S.C. § 512(a)-(d).

In affording distinct treatment of service providers based upon the particular functions they are performing, Title II recognizes a longstanding distinction in the law of copyright—the difference between: i) an entity acting as a passive conduit for communications created, controlled, stored, and disseminated by others; and ii) an entity storing or "hosting" material on its own system or network and itself disseminating that material to others. *Compare id.* § 512(a)

("Transitory Digital Network Communications"), *with id.* § 512(c) ("Information Residing on Systems or Network at Direction of Users"). Entities performing the former pure "transmission" or "conduit" function, such as telephone companies, have traditionally enjoyed immunity from liability for contributory infringement. *See, e.g., E. Microwave, Inc. v. Doubleday Sports*, 691 F.2d 125, 128 (2d Cir. 1982) (discussing historical "common carrier" immunity for copyright infringement); P. Huber, *et al.*, Federal Telecommunications Law 1240-55 (2d ed. 1999). Subsection (a) of Section 512, which describes the "transmission" or "conduit" function for an Internet service provider, mirrors this traditional immunity and is not conditioned on the performance of *any independent duties* by service providers.

By contrast, subsections (b), (c), and (d) of Section 512, which pertain to circumstances in which the service provider plays a relatively more active role, condition the service provider's DMCA protection on its performance of specific duties to assist copyright owners in protecting their property interests. These duties apply only in situations where the service provider has the ability to locate the particular material claimed to be infringing and to either selectively remove it or temporarily disable access to it via the Internet. In the context of subsections (b), (c), and (d), the service provider itself is storing and controlling the dissemination of some potentially infringing material on its own system or network, and—unlike the service provider who functions as a mere conduit as described in subsection (a)—has both the technical ability and the legal right to locate and alter or disable Internet access to particular material.

Subsection (c) of the statute addresses the paradigmatic situation where the service provider has substantial control over potentially infringing material. It applies to "material that resides on a system or network controlled or operated by or for the service provider," *id.* § 512(c), such as a website "hosted" on a service provider's servers. Subsection (c) establishes a "notice and take-down procedure" by which a copyright owner may notify a service provider

that material it is hosting is potentially infringing, *see id.* § 512(c)(3), and thereby require the service provider, as a condition of receiving limited immunity, to "remove, or disable access to, the material that is claimed to be infringing," *id.* § 512(c)(1)(C). The notification must specify a particular "online site" where the allegedly infringing material is located and must contain: "[i]dentification of the material that is claimed to be infringing . . . and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material." *Id.* § 512(c)(3)(A)(ii) & (iii).

The statute makes quite clear that the physical "remov[al]" of "material" or "disabling access" to "material" is a different remedy from the "termination" of a subscriber's "account." The former remedy is surgical and involves excising particular material from a website or temporarily disabling access to the material. By contrast, termination of a subscriber's account involves ending the subscriber's ability to gain any access to the Internet through that account. Subsections (j) and (i) of the statute both distinguish between these two concepts, describe them in different terms as applying to different things (*e.g.*, "material" versus "subscribers" or "accounts"), and establish very different predicates for their use. *Compare id.* § 512(j)(1)(A)(i) (authorizing injunction restraining service provider "from providing access to infringing material"), *with id.* § 512(j)(1)(A)(ii) (authorizing injunction restraining service provider "from providing access to a subscriber or account holder . . . by terminating the accounts of the subscriber or account holder"); *see also id.* § 512(i) (providing for "the termination of subscribers and account holders of the service provider's system or network who are repeat infringers").

Subsections (b) and (d) deal with storage functions where the service provider has less control over the content and correspondingly more limited duties as a precondition to statutory immunity. Subsection (b) addresses "caching," where a service provider's system automatically makes a copy of a website that is hosted elsewhere in order to facilitate ready access by its customers. Subsection (d) deals with information location tools, such as

"a directory, index, reference, pointer, or hypertext link" that refers or links users to potentially infringing material. Both subsections (b) and (d) make explicit cross-reference to the "notice and take-down procedure" established by subsection (c) and incorporate modified versions of that procedure into the service provider's duties under those subsections. *Id.* § 512(b)(2)(E), (d)(3).

Numerous provisions of Section 512, including the subpoena provision at issue in these proceedings, expressly cross-reference or incorporate concepts from the "notice and take-down" procedures established in subsection (c)(3). Thus, subsection (f) provides for damages and attorney's fees where a misrepresentation in a subsection (c)(3) notification results in the erroneous removal of or disabling of access to non-infringing material. Subsection (g) establishes a procedure for "counter notification" by the individual associated with the material that is the subject of a subsection (c)(3) notification and, unless certain conditions are met by the copyright owner, requires the service provider to restore access to the removed or disabled material. Finally, and as discussed in detail below, subsection (h), the subpoena provision at issue here, incorporates the subsection (c)(3) "notice and take-down procedure" at every stage of the subpoena process.

Subsection (a) thus stands alone among the operative provisions of the statute in that it does not provide for any notification and take-down procedure and it does not make any reference to the notice and take-down procedures contained in subsection (c)(3). In fact, subsection (a) does not impose any duties on service providers to remove or disable access to any material.

What the structure of the statute implicitly establishes both the statutory text and legislative history make explicit—the particular functions service providers are performing drive the application of all the service provider duties contained in the statute. *See id.* § 512(n) ("Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section."); S. Rep. No. 105-190, at 19 (1998) ("In the beginning, the Committee identified the following activities: (1) digital network

communications, (2) system caching, (3) information stored on service providers, and (4) information location tools.").

Subsection (h) contains the novel subpoena provision at issue here. This provision permits a copyright owner or its representative, under very specific circumstances, to obtain a subpoena to force a service provider to turn over identifying information about a subscriber associated with specific allegedly infringing material. Consistent with the organization of Title II as a whole, subsection (h)'s application is dependent entirely on which function the service provider is performing.

Specifically, subsection (h) incorporates and relies upon the notification procedures applicable to subsections (b), (c), and (d) at each stage of the subpoena process. Subsection (h)(2), entitled "Contents of request," mandates that "a copy of the notification described in subsection (c)(3)(A)" be filed with the clerk of the court with any request for a subpoena. Subsection (h)(3), entitled "Contents of subpoena," specifies that the subpoena shall "authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose . . . information sufficient to identify the alleged infringer of the material described in the notification." Subsection (h)(4), entitled "Basis for granting subpoena," provides that, "[i]f the notification filed satisfies the provisions of subsection (c)(3)(A)" and other conditions precedent, the clerk must issue and sign the proposed subpoena. Finally, subdivision (h)(5), entitled "Actions of service provider receiving subpoena," requires that "a notification described in subsection (c)(3)(A)" be served upon the service provider either with or before any DMCA subpoena.

That Congress chose to tie the subpoena provision—and the correlative duty of the service provider to disclose its subscriber's identity—to storage functions, and to the "notice and take down" procedures that are applicable only to storage functions, is not surprising. It reflects the fact that in 1998, the central problem Congress addressed was the unlawful dissemination of copyrighted material through websites hosted by service providers. The primary

remedy in the DMCA (besides copyright owner self-help that does not involve the service provider) was the take-down procedure, which is designed to "remove" particular material that is claimed to be infringing from a website or "disable access" to material pending the further procedures specified in subsection (g).

The personal communications from one Internet user to another were not viewed as a major threat to copyright holders' interests in 1998. First, peer-to-peer software, which now allows for the identification and transmission of digital files from one Internet user's computer to another's, simply did not exist in 1998. Pet. 14a-15a, 42a. Peer-to-peer software, such as "KaZaA" and "Grokster," that allows each computer to be both server and client and to search and download material from users' hard drives without utilizing a central server or directory did not arrive on the scene until after the legal demise of Napster in 2000.[1]

Second, in 1998, the vast majority of individual Internet users were limited to dial-up connections at speeds that simply did not allow for the instantaneous exchange of large digital files, such as music files in MP3 format. *See, e.g., Inquiry Concerning the Deployment of Advanced Telecommunications Capability*, 14 F.C.C.R. 2398, ¶¶ 6, 16 (1999) (broadband services at "an early stage of deployment"; only a "fledgling market" for them existed).

In addition, the limited reach of the DMCA's novel subpoena provision reflects the fact that Congress viewed those subsection (a) functions that did exist in 1998, such as email and web browsing, H.R. Rep. No. 105-551, at 42 (1998), as private

1. *See Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. (Sept. 9, 2003) (Statement of John Malcolm, U.S. Dep't of Justice) (distinguishing the vastly different "fisherman's net" architecture of peer-to-peer applications from the "traditional networks" in place in 1998 where "people who want[ed] to share files . . . stored them on one or more central 'servers'").

expressive activities not to be disturbed by *any* provision of the DMCA.[2] The distinction between information stored on an external network (*e.g.*, the service provider's network or system), *see* 17 U.S.C. § 512(c), and information stored on an individual's home computer, *see id.* § 512(a), reflects the higher level of subscriber privacy expectations when an Internet user stores information on a home computer or engages in other activities that do not require storage on a public server. It reflects, too, the difference between burdening service providers with the role of "copyright policeman," requiring them to invade their subscribers' privacy in the name of any private copyright enforcement efforts, and requiring service providers to exercise narrowly targeted, content-specific control over material resident on their own systems. *Id.* § 512(m)(1).

2. The Two Subpoenas at Issue in These Proceedings

RIAA caused the issuance of two subpoenas by the United States District Court for the District of Columbia under the purported authority of Section 512(h). The subpoenas were served on Verizon on July 24, 2002 and February 4, 2003. The subpoenas commanded Verizon to disclose to RIAA, under penalty of contempt, the names, addresses, and telephone numbers of two of its otherwise anonymous subscribers. RIAA claimed that Verizon's subscribers were "using Verizon's network to offer for downloading copyrighted songs through peer-to-peer software provided by KaZaA, without the copyright holders' authorization." Pet. 23a, 56a-57a.

---

2. In Title I, Congress recognized that copyright holders' use of "self-help" technologies to monitor infringement could potentially interfere with individuals' privacy on their home computers and, therefore, enacted a "Savings clause" to protect consumer privacy. 17 U.S.C. § 1205. And, in what is codified as 17 U.S.C. § 512(m) and entitled "Protection of Privacy," Title II of the DMCA makes clear that nothing in Section 512 should be construed to require a service provider to monitor its subscribers' private communications.

B. The Proceedings Below

1. The District Court's Decisions

Verizon refused to reveal its subscribers' identities to RIAA. In the first proceeding, RIAA filed a motion to enforce the subpoena, and Verizon objected on the ground that Section 512(h) does not apply to situations in which a service provider is merely performing a conduit function as described under Section 512(a).

The district court rejected Verizon's arguments, holding that the subpoena power applied to every form of expression on the Internet, including those where no potentially infringing material resides on a service provider's system or network. Pet. 26a-44a. The district court conceded that peer-to-peer file-sharing software, such as a KaZaA, was "'not even a glimmer in anyone's eye when the DMCA was enacted' by Congress in 1998." *Id.* at 42a. It nonetheless concluded that Section 512(h) should be extended to apply to situations where the service provider is performing conduit functions to avoid creating what it characterized as a "huge loophole" in the statute. *Id.* at 36a. The district court also believed that the general definition of "service provider" contained in subsection (k) of the statute was relevant to the issue of what duties are imposed by particular subsections of the statute. *Id.* at 26a-30a. Based upon these observations, the district court ordered Verizon to comply with the July 24, 2002 subpoena. *Id.* at 54a.

In the second proceeding, Verizon filed a motion to quash the February 4, 2003 subpoena on the grounds that it was issued and would be enforced outside of any "case or controversy" within the jurisdiction of the federal courts under Article III and that the bare assertion of a "good faith belief" of infringement in an *ex parte* filing with the clerk provided insufficient protection of Internet users' First Amendment rights. The district court denied Verizon's motion and ordered Verizon to comply with the February 4, 2003 subpoena. Pet. 55a-111a.

---

2. The Court of Appeals' Reversal of the District Court

With Chief Judge Ginsburg writing for a unanimous panel, the D.C. Circuit "agree[d] with Verizon's interpretation of the statute" and reversed the district court's judgments in both subpoena proceedings.[3] Pet. 2a. The court of appeals "conclude[d] from both the terms of § 512(h) and the overall structure of § 512 that . . . a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity." *Id.* at 6a. Because the D.C. Circuit agreed with Verizon's interpretation of the statute, it did not reach either of the constitutional arguments that were pressed and passed upon below and fully briefed on appeal. *Id.* at 2a.

First, the D.C. Circuit "agree[d] with Verizon that § 512 does not *by its terms* authorize the subpoenas issued" where Verizon was performing only the "conduit" functions addressed in Section 512(a). *Id.* at 12a (emphasis added). The court recognized that there are "three items" a copyright owner "must file . . . along with its request that the Clerk of a district court issue a subpoena," the first of which is "a 'notification of claimed infringement' identifying the copyrighted work(s) claimed to have been infringed and the infringing material or activity, and providing information reasonably sufficient for the ISP to locate the material, all as further specified in § 512(c)(3)(A)." Pet. 4a. Specifically, the notice must "identify material 'to be removed or access to which is to be disabled'" by the service provider. *Id.* at 9a (quoting 17 U.S.C. § 512(c)(3)(A)(iii)).

The court of appeals noted that "§ 512(h)(4) makes satisfaction of the notification requirement of § 512(c)(3)(A) a condition precedent to issuance of a subpoena." Pet. 9a. Because the material involved in peer-to-peer exchanges is located "in the computer (or in an off-line storage device, such as a compact disc) of an individual user," the service provider "can not remove or disable

---

3. The district court treated the two subpoena enforcement proceedings as "related matters," and its second decision applied to both cases. The court of appeals then consolidated both appeals for purposes of briefing, argument, and disposition.

one user's access to infringing material resident on another user's computer." *Id.* at 9a-10a. Nor, given the clear distinctions drawn in subsection (j), could the concept of removing or disabling access to particular material be equated with the different remedy of termination of a subscriber's account. *Id.* at 10a. Because the condition precedent to issuance of a subpoena can *never* be satisfied in the subsection (a) setting, the court of appeals reasoned that the subpoena provision itself must not apply to conduit functions. *Id.* at 11a.

Second, the court of appeals emphatically rejected both the district court's and RIAA's reliance on the definition of "service provider" in Section 512(k)(1)(B), an argument that continues to figure prominently in RIAA's petition. Pet. 19-21. The court of appeals candidly stated that this argument "borders upon the silly," *id.* at 11a, and went on to expose its fallaciousness in pointed terms:

> The details of this argument need not burden the Federal Reporter, for the specific provisions of § 512(h), which we have just rehearsed, make clear that however broadly "[internet] service provider" is defined in § 512(k)(1)(B), a subpoena may issue to an ISP only under the prescribed conditions regarding notification. Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A).

Id. at 11a-12a.

Third, the D.C. Circuit analyzed the *structure* of Section 512 as a whole, and in particular the difference between the storage functions addressed in subsections (b) through (d) and the distinct transmission function covered by subsection (a). The court explained that Section 512(h)'s three cross-references to Section 512(c)'s notice requirement could be given meaning and effect in the context of subsections (b), (c), and (d), but *could not be given any meaning or effect in the context of subsection (a)*. *Id.* at 12a-14a. The court thus concluded that "the references to § 512(c)(3)"

in subsections (b) through (d) "lead inexorably to the conclusion that § 512(h) is structurally linked to the storage functions of an ISP and not to its transmission functions, such as those listed in § 512(a)." *Id.* at 14a.

Fourth, the D.C. Circuit found that it

> need not . . . resort to investigating what the 105th Congress may have known because the text of § 512(h) and the overall structure of § 512 *clearly establish* . . . that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others.

Id. at 14a (emphasis added). Nonetheless, the D.C. Circuit did examine RIAA's proffered "legislative history" and concluded that, "the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works." *Id.* Quite simply, the court concluded: "Congress had no reason to foresee the application of § 512(h) to [peer-to-peer] file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along." *Id.* at 15a.

Finally, the D.C. Circuit rejected RIAA's invitation to "rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been to the music industry." *Id.* at 16a. The court invoked this Court's teaching in *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), and held that "[t]he plight of copyright holders must be addressed in the first instance by the Congress" because "only the 'Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.'" Pet. 16a (quoting *Sony*, 464 U.S. at 431).

REASONS FOR DENYING THE PETITION

I. The Petition Meets None Of The Established Justifications For Intervention By This Court.

A. There Is No Split of Authority on the Narrow Statutory Issue Resolved by the D.C. Circuit.

More than four years after the DMCA was enacted, RIAA brought these proceedings, admittedly as "test case[s]," Pet. 19a, to advance a novel and expansive interpretation of the scope of Section 512(h). RIAA concedes that the D.C. Circuit is the first court of appeals in the nation to address the scope of the DMCA's unique subpoena provision. Pet. 14. Thus, RIAA can lay claim to no conflict with the decisions of this Court or *any* appellate court, state or federal. In fact, not only is the D.C. Circuit the first appellate court to construe this particular statutory provision, but RIAA itself candidly acknowledges that the "identical issues" are now being considered in other circuits. *Id.*

Just this month, the Eighth Circuit heard oral argument in *RIAA v. Charter Communications, Inc.*, No. 03-3802 (8th Cir.), to determine whether the district court in that case erred in enforcing a DMCA subpoena where the service provider was performing only the "conduit functions" specified in Section 512(a). The same legal issues are also now before a district court in the Fourth Circuit, where the parties completed briefing last month and are awaiting the district court's decision in the context of motions to quash filed by the Internet subscribers themselves. *In re Subpoena to Univ. of N.C.*, No. 1:03mc138 & *In re Subpoena to N.C. State Univ.*, No. 1:03mc139 (M.D.N.C.).

In short, there is not now and there may never be any conflict in the circuits or confusion over the meaning of this statutory provision. At a minimum, this Court should allow continuation of the normal process whereby multiple circuits are encouraged to address a novel legal issue before any intervention by this Court. Whether even an intercircuit conflict would warrant review—where Congress is best suited to conduct, and actively interested in conducting, the careful

fact-intensive policy examination of new circumstances needed for forward-looking resolution—can be left for another day.

B. No Extraordinary Circumstances Justify Review.

This case presents no issue of immediate public importance that would itself justify review. RIAA's implication that the urgency of the "social problem," Pet. 17, of peer-to-peer file sharing demands review is belied by RIAA's own actions in the wake of the D.C. Circuit's decision. Far from being left without the ability to "fight back," RIAA has available to it, and *has extensively and successfully utilized*, the so-called "John Doe" procedure for identifying alleged infringers.

The filing of a John Doe suit, along with a motion for third-party discovery of the identity of the defendant "John Doe" is the traditional means to invoke the power of the federal courts against an otherwise anonymous defendant. Armed with this alternative legal tool, a month after the D.C. Circuit issued its decision, RIAA President Cary Sherman was able confidently to announce that RIAA's "campaign against illegal file sharers *is not missing a beat*. . . . [W]e can and will continue to bring lawsuits on a regular basis against those who illegally distribute copyrighted music." Jan 21, 2004 RIAA Press Release, *at* http://www.riaa.com/news/newsletter/012104.asp (visited June 21, 2004) (emphasis added).

Since the D.C. Circuit opinion issued, the recording industry has filed "John Doe" lawsuits against more than 3,000 alleged infringers, in well over a dozen district courts across the country. As a direct result of those efforts, RIAA has settled disputes with approximately 600 individuals, *see* John Borland, *RIAA takes hundreds more 'John Does' to court*, CNET News.com (June 22, 2004), *at* http://zdnet.com.com/2102-1104_2-5243587.html? (visited June 22, 2004), and its members have proceeded with lawsuits against named individuals who did not settle, some of which already have resulted in awards of infringement damages and permanent injunctions. *See, e.g., Arista Records, Inc. v. Brothers*, No. 3:03cv2081(JCH) (D. Conn. Apr. 30, 2004).

Moreover, since the advent of these John Doe cases, Mr. Sherman has publicly stated that RIAA has "seen a marked decline in illegal file-sharing, a marked increase in business at the legitimate online music services, and a spike in CD sales as well." Mar. 25, 2004 Transcript of Q&A With RIAA President Cary Sherman, *at* http://www.dailytexanonline.com/news/2004/03/25/Focus/Transcript.Of.Qa.With.Riaa.President.Cary.Sherman-641217.shtml (visited June 14, 2004). RIAA's preference for one legal tool over another in protecting the business interests of its members is not the kind of national legal crisis that warrants a grant of certiorari.

C. RIAA's Policy Arguments Regarding New Technologies and Requests To Expand Copyright Protections Are Properly Addressed to Congress, Not to this Court.

The D.C. Circuit did not, as RIAA suggests, strike down a federal statute or "gut[]" or "blow[] a hole in" the DMCA's subpoena provision. Pet. 15, 19, 27. The court engaged in a routine exercise in statutory construction, focusing on the plain language of the subpoena provision, its place in the statutory scheme as a whole, and the state of Internet technology and evidence regarding the scope of the problem Congress believed it was addressing in 1998. None of these traditional tools of statutory construction even hinted that the subpoena provision was written or intended to address the new problem of peer-to-peer file sharing as it exists today. Nothing in the court of appeals' opinion prevents copyright owners or their agents from using both the "take down" and subpoena provisions for all the functions addressed in subsections (b), (c), and (d).

At bottom, RIAA is asking this Court to alter the words of the subpoena provision, the structure of Section 512 as a whole, and the balance among the rights of copyright holders, Internet service providers, and Internet users that Congress struck based upon the evidence before it in 1998. The court of appeals and the district court both agreed on one historical fact that no amount of RIAA revisionist history can change: "[T]he legislative history of the DMCA

betrays no awareness whatsoever that internet users might be able to directly exchange files containing copyrighted works. That is not surprising; P2P software was 'not even a glimmer in anyone's eye when the DMCA was enacted.'" Pet. 14a (quoting Pet. 42a).

As the D.C. Circuit properly recognized, the job of expanding copyright protections in light of new technologies is uniquely the province of Congress, which has the institutional competence to engage in meaningful fact-finding and to balance the competing interests implicated by peer-to-peer file-sharing. Pet. 16a. Indeed, faced with the record that has unfolded since Congress first enacted the DMCA—including, *inter alia*, the susceptibility of the DMCA subpoena process to mistakes (through human error or the use of pre-programmed robotic tools to search for alleged infringement), and abuse of the process by alleged copyright owners that are significantly less responsible than RIAA[4]—it is far from a forgone conclusion that Congress would place the interests of copyright owners in a streamlined subpoena tool over the interests of Internet

---

4. The record below is filled with evidence of mistakes by copyright owners and their representatives and examples of potential abuses of the cursory DMCA subpoena process. One copyright bounty hunter mistook a file entitled "Harry_Potter_Book_Report.rtf" for an infringing copy of the movie *Harry Potter and the Sorcerer's Stone.* The file was in fact a child's book report, but the robotic program the bounty hunter used to search the Internet for potential copyright infringement could not tell the difference. In the proceedings below, RIAA even submitted a sworn declaration of a pornography purveyor, ALS Scan, who averred to its use of the DMCA subpoena process in protecting its copyrighted works. *See* http://www.alsscan.com/copyright.html (claiming copyright in hundreds of pornographic images). After the case was submitted to the D.C. Circuit, RIAA obtained and executed a DMCA subpoena based upon its "good faith belief" that a subscriber had downloaded over 2,000 songs, and then filed an infringement action against the identified subscriber seeking damages of up to $150,000 per song. As it turned out, the defendant, whose privacy and anonymity were improperly breached, was a 66-year-old grandmother who does not even own a computer capable of running file-sharing software. *See* Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sept. 24, 2003, C1.

users in protecting their privacy in communications stored on their home computers.

Copyright owners repeatedly have sought to have the federal courts "adapt" existing law to cover new technologies that *they perceive* as a threat to their business interests. This Court has repeatedly declined such invitations, finding that the adjustment of rights necessary where new technologies alter the market for copyrighted works is, as a matter of both textual commitment and institutional competence, for Congress alone to decide:

> Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.

Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).

Just last Term, this Court reiterated its commitment to "defer substantially to Congress" on copyright issues and reaffirmed that "it is generally for Congress, not the courts, to decide how best to pursue the Copyright Clause's objectives." *Eldred v. Ashcroft*, 537 U.S. 186, 204 (2003) (citing *Sony*, 464 U.S. at 429, and *Stewart v. Abend*, 495 U.S. 207, 230 (1990)). Consistent with this well-established principle of judicial restraint in the copyright field, this Court should decline RIAA's invitation to use a statute that is almost six years old to wade into an ongoing legislative debate about how to address the latest developments in Internet technology. The issue should be left with Congress, which, as the D.C. Circuit noted, Pet. 16a, is presently conducting hearings regarding peer-to-peer technologies and considering possible legislative responses to them.

II. The Court Of Appeals Correctly Applied Settled Canons Of Statutory Construction.

A. The Text, Structure, History, and Purpose of Section 512 Compel the Result Reached by the D.C. Circuit.

A unanimous panel of the D.C. Circuit correctly resolved what RIAA itself describes as "a straightforward issue of statutory construction." Pet. 17. Try as it might, RIAA is unable to offer this Court a coherent and logical interpretation of subsection (h) in particular, or of Section 512 in general, that is consistent with its litigation position. The statute can only get RIAA where it wants to go through a less than subtle form of result-oriented bending and twisting that runs counter to basic canons of statutory construction. In the end, RIAA's arguments fail even to address, let alone cast doubt upon, the court of appeals' careful statutory analysis.

1. The Text and Structure of Section 512 Compel the Conclusion That Section 512(h) Applies Only to Material Stored on a Service Provider's System or Network.

Under the plain language of Section 512(h), the issuance of a subpoena to compel a service provider to disclose confidential information about its subscriber's identity is conditioned on the filing and service of a valid take-down notification described in subsection (c)(3)(A). Thus, the scope and application of subsection (h) is dependent on: i) whether the notification and take-down procedure applies to the particular function at issue; and ii) whether both the copyright owner and the service provider can comply with the requirements of, and obligations created by, the notice and take down procedure as specified in subsection (c)(3)(A).

On its face, subsection (h) contains three separate cross-references to the subsection (c)(3)(A) take-down notice, 17 U.S.C. § 512(h)(2)(A), (h)(4), (h)(5), and expressly makes "satisf[action of] the provisions of subsection (c)(3)(A)" a condition precedent to the issuance of every Section 512(h) subpoena, *id.* § 512(h)(4). In turn, the required subsection (c)(3)(A) notice, the statute says, can "be effective" only if it allows the service provider to "locate"

and "remove" or "disable[]" "access to" "the material that is claimed to be infringing." *Id.* § 512(c)(3)(A)(iii).

As the D.C. Circuit concluded, these statutory requirements for the issuance of a Section 512(h) subpoena cannot have any force or effect in the subsection (a) context. The statute does not authorize any subsection (a) take-down notices, and a service provider performing conduit functions under subsection (a) has neither the technical ability nor the legal right to locate and selectively remove or disable Internet access to material residing on the personal computers of individual subscribers. Pet. 9a-10a.

In order to accept RIAA's reading of the statute (*i.e.*, that subsection (h) applies regardless of the service provider's function), one must ignore the fact that Congress omitted any notice and take-down provisions from subsection (a). RIAA's construction renders Section 512(h)'s numerous cross-references to *material* that is the subject of a subsection (c)(3)(A) notice (material which the service provider must be able to locate, remove, or disable access to) so much congressional gibberish because that kind of material can never exist in the subsection (a) context. Under RIAA's reading of the statute, Congress required the filing and service of a meaningless document that could never "satisf[y] the provisions of subsection (c)(3)(A)," *id.* § 512(h)(4), and could never obligate the service provider to do anything. In addition, the damages remedy for a misrepresentation that particular material is infringing in subsection (f) applies only where the service provider is able to remove or disable access to the material and thus would *never* apply to representations made to obtain a subpoena in the subsection (a) context. The limits on this important protection for subscribers further confirms that Congress was addressing only storage functions in subsection (h). The only coherent reading of Section 512(h) is that its cross-references to subsection (c)'s take-down notice *do* have meaning and effect, because

Section 512(h) applies only to storage functions where a take-down notice is provided for and can be effective.[5]

While the D.C. Circuit carefully adhered to this Court's instructions regarding holistic construction of statutes to arrive at a logical and harmonious whole, *see, e.g., FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), the petition quite consciously eschews this approach and instead attempts to poke holes in the D.C. Circuit's opinion by reading isolated statutory provisions out of context. Each one of these attempts is futile.

First, RIAA argues that the D.C. Circuit erred when it determined that a service provider performing conduit functions under subsection (a) is unable to "remove" or "disable access to" the allegedly offending material. Pet. 22-23. In support of this theory, RIAA posits that the service provider in the subsection (a) context could, *in lieu of* removing or disabling access to the content at issue, terminate the subscriber's account entirely, thereby preventing the subscriber from sending or receiving *any content at all* over the Internet. *Id.*

Not only does this suggestion impute to Congress an implausible intent to require the radical step of termination of all Internet access based only upon an *ex parte* assertion of a "good faith belief" that some material may be infringing, it also ignores the care with which Congress distinguished between requiring a service provider surgically to remove or disable access to particular material and the altogether different remedy of requiring a service provider to terminate a subscriber's account. *See* 17 U.S.C. § 512(j)(1)(B)(i) (referring to injunctive relief that requires "terminating the accounts of the subscriber"). To ignore this distinction is to violate the elementary canon of statutory interpretation that different words in

---

5. A statutory cross-reference is a well-recognized mechanism for incorporating procedures or limitations from another part of the same statute. *E.g., Overseas Educ. Ass'n v. FLRA*, 824 F.2d 61, 65 (D.C. Cir. 1987); *Estate of Joseph Leder v. Comm'r of Internal Revenue*, 893 F.2d 237, 241 (10th Cir. 1989).

the same statute are to be interpreted differently. *Williams v. Taylor*, 529 U.S. 362, 404 (2000).

It is no answer that statutory terms can have "overlapping" meanings. Pet. 22-23 & n.16. The general proposition that some overlap of statutory terms is theoretically possible says nothing about the correct interpretation and interrelationship of the specific terms used in Section 512. Even if overlap exists, it does nothing to undermine the distinct nature of the terms as employed in the relevant provisions of this statute.[6] Thus, compared with removing or disabling access to material, which the service provider can do in a precise manner when it hosts that material, and which the service provider may have a further obligation to undo under subsection (g), termination of a subscriber's account is often a broader remedy—ending the subscriber's ability to send or receive any material over the Internet. Pet. 10a. It could also be viewed as a narrower remedy in the sense that it may not remove access to particular material at all if the subscriber has another means of Internet access to receive or disseminate that material. Many terms in the English language have some conceptual overlap, but that general proposition cannot undermine a specific choice by Congress in a particular statute to invoke one term or concept in some places and another term or concept in others.

In Section 512, the termination of accounts is referenced in several places, *see* 17 U.S.C. § 512(j)(1)(A)(ii), (j)(1)(B)(i), (i)(1)(A), but never in the context of a take-down notice or the

---

6. Indeed, even within subsection (j) itself, Congress distinguished between "[a]n order restraining the service provider from providing access to *infringing material or activity* residing at a particular online site on the provider's system or network," 17 U.S.C. § 512(j)(1)(A)(i) (emphasis added), and one "restraining the service provider from providing access to a subscriber . . . of the service provider's *system or network* who is engaging in infringing activity . . . , by terminating the accounts of the subscriber," *id.* § 512(j)(1)(A)(ii) (emphases added). Moreover, Congress reserved the extreme remedy of account termination for repeat infringers or those subject to a court order. *Id.* § 512(i), (j). No such remedy is provided for "alleged infringers," *id.* § 512(h)(1), who can be the subject of Section 512(h) subpoenas.

subpoena provision. By contrast, the terms "remove" and "disable access" are used exclusively in provisions that address storage functions, where the service provider has access to and control of the material at issue. *See, e.g.*, § 512(b)(2)(E), (c)(1)(C), (c)(3)(A)(iii), (d)(3), (f)(2), (g)(1)&(2). The removal of or disabling of access to particular material cannot be equated with the termination of a subscriber's account without doing violence to both the text and structure of the statute.

Second, RIAA argues that the D.C. Circuit's reading of the subpoena provision "is contradicted by" subsection (h)(5). Pet. 21-22. Subsection (h)(5) not only fails to support RIAA's position but provides *further proof* that the subpoena provision does not apply to the subsection (a) context. Subsection (h)(5) includes one of the three express cross-references to the notification in subsection (c)(3)(A) and states that, "[u]pon receipt of the issued subpoena . . . , the service provider shall" disclose the information sought, "regardless of whether the service provider responds to the notification." 17 U.S.C. § 512(h)(5).

To the extent this last clause of subsection (h)(5) bears on the content or effect of the notification at all, it undermines RIAA's position because the negative implication of the clause is that subpoenas will be issued only in circumstances where a service provider *could* effectively respond to the notification, even if it chooses not to do so. Subsection (h)(5) also contemplates that a take-down notification might be served *before* a subpoena, which of course makes no sense if the take-down notice is purely "informational" and its only purpose is to obtain the subpoena. Pet. 21-22.

Finally, RIAA posits that the D.C. Circuit erred by not giving adequate weight to the definition of "service provider" in the statute. Pet. 20-21. The use of the generic definition of "service provider" in 512(h) simply means no service provider is excluded from Section 512(h) at the threshold definitional level. It is a non sequitur to say that, for that reason, a subpoena can be issued under Section 512(h) when the provision's express *requirements* are not met.

Those requirements, as described, include the hosting requirement. RIAA's argument, the D.C. Circuit correctly concluded, "borders upon the silly." Pet. 11a.

2. The Legislative History and Purpose of the Statute Further Confirm That Section 512(h) Does Not Apply to the Conduit Context.

This is a case where "the plain language" of the DMCA should "mark[] the beginning and end" of the judicial inquiry. *U.S. R.R. Ret. Bd. v. Fritz*, 449 U.S. 166, 176 (1980). Unable to reconcile its preferred interpretation with the text and structure of Section 512, RIAA devotes the bulk of its petition to arguing that Congress could not possibly have intended to limit the subpoena provision to storage functions and that adhering to the plain language and structure of the statute frustrates congressional purpose (as now defined by RIAA more than four years after the statute was enacted). Pet. 15-19, 23-24.

RIAA cannot deny that the peer-to-peer architecture was not contemplated by Congress in 1998 and instead relies on scattered snippets of congressional testimony, generally drawn from spokespersons for copyright owners or from discussions of legislation *other than the DMCA*[7] to suggest that Congress had some premonition about copyright problems that could arise in the conduit context. Not only are the self-serving statements of copyright owners a poor guide to statutory interpretation, *see, e.g., S&E Contractors, Inc. v. United States*, 406 U.S. 1, 13 n.9 (1972), but even those statements RIAA has chosen to

---

7. *See, e.g.*, Pet. 3-4 (citing to hearings regarding an amendment to the criminal provisions of the Copyright Act that had nothing to do with service provider duties under Title II of the DMCA); *id.* at 6 (same); *id.* at 6 n.8 (statement of songwriter); *id.* at 8 n.11 (quoting testimony of RIAA's General Counsel). RIAA also cites pre-enactment news articles that it claims discuss technologies antecedent to peer-to-peer file sharing. *E.g.*, Pet. 4-5. These news reports may reflect what technology experts were anticipating in the development of Internet technologies, but they offer no support for the proposition that Congress considered, let alone attempted to address, these issues in 1998.

highlight do not connect the subsection (a) functions to the subpoena provision.[8]

Finally, RIAA argues that the views of the Register of Copyrights, expressed in a legislative hearing five years after the DMCA was enacted, are "entitled to deference." Pet. 16 & n.14. This is interpretive desperation. The Register has been delegated no authority to interpret or apply Section 512(h), and her testimony relies on RIAA's and the district court's flawed interpretation of Section 512(h). Thus, the Register's testimony on this issue of statutory construction is not entitled to any weight in this Court. *See, e.g., United States v. Mead Corp.*, 533 U.S. 218, 227, 231 (2001); *Christensen v. Harris County*, 529 U.S. 576, 587 (2000).

B. The D.C. Circuit's Reading of the Statute Avoids Serious First Amendment Concerns.

Because the D.C. Circuit agreed with Verizon's position that the subpoena provision does not apply to the conduit context, the court properly declined to reach the First Amendment issues decided by the district court. Pet. 2a. To the extent there is any doubt as to whether the subpoena provision should be read to apply to the conduit context, the D.C. Circuit properly avoided the serious First Amendment concerns presented by an expansive reading of this unique subpoena power.

As the district court correctly concluded, Pet. 79a-82a, there can be no doubt that Internet users have a First Amendment right to speak and associate anonymously. *See, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995). By design, at the time Section 512(h) is invoked, there has been no judicial determination of copyright infringement and thus the Internet speaker

---

8. Indeed, the only testimony of the type RIAA draws upon that connects the sharing of information about "the infringer's identity" to a particular function ties it to "material [located at] a particular site on a service provider's system." *Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 105th Cong. 77 (1997) (statement of Robert W. Holleyman II, President, Business Software Alliance).

who is the subject of the subpoena must be presumed to be engaged in fully protected speech and association. Because Section 512(h) is a procedure designed to strip Internet users of this presumptively protected anonymity, "those procedures violate the First Amendment unless they include built-in safeguards against curtailment of constitutionally protected expression, for Government 'is not free to adopt whatever procedures it pleases for dealing with [illicit content] without regard to the possible consequences for constitutionally protected speech.'" *Blount v. Rizzi*, 400 U.S. 410, 416 (1971).[9]

Section 512(h) on its face includes no such protections and, under RIAA's reading, would permit the employment of a federal court's power to strip Internet users of their anonymity upon no more than an *ex parte*, subjective "good faith" statement by anyone willing to claim that he or she is a copyright owner or the owner's representative and that some form of copyright infringement *might* be occurring. 17 U.S.C. § 512(c)(3)(A)(v). Such a cursory showing is not sufficient to shift the burden to the service provider (who does not even have access to the material) to defend the First Amendment rights of its subscriber. *See, e.g., Blount*, 400 U.S. at 418. Under any level of First Amendment scrutiny, this process fails the requirement that laws restricting speech be narrowly tailored to impose the least burden on protected speech and that the advocate of suppression of speech or association bear the burden of proof. *Freedman v. Maryland*, 380 U.S. 51, 58-60 (1965); *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 775-78 (1986).

Finally, even if these serious First Amendment concerns did not raise doubts about the subpoena provision as a whole, they further support the D.C. Circuit's conclusion that subsection (h) does not apply to the conduit context. Under the D.C. Circuit's reading, those activities where the subscriber's privacy and anonymity interests

---

9. It is for this reason that federal courts have demanded that those who would seek to strip Internet users of their anonymity must not merely file a complaint, but also must demonstrate that their allegations can withstand heightened judicial scrutiny. *E.g., Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 579-80 (N.D. Cal. 1999).

are at their zenith, in connection with material stored on the subscriber's own home computer, are not subject to Section 512(h)'s truncated process. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (expressive activity that may be proscribed outside the home is constitutionally protected inside the home). In addition, where the material resides on the service provider's system or network, the service provider can examine the material and come to a judgment about the infringement claim. Finally, only in the context of an effective take-down notice are the protections of subsections (f) and (g) available to the subscriber. The fact that the D.C. Circuit's reading of the statute comports with *both* traditional canons of statutory construction *and* principles of constitutional avoidance confirms that this Court's review is neither necessary nor likely to lead to a different outcome.

C. The Existence of a Substantial Alternative Ground for Affirming the Judgment Below Militates Against Granting the Petition.

Because it agreed with Verizon's reading of the statute, the court of appeals did not address another issue that was decided by the district court and fully briefed on appeal—the question whether the issuance of these subpoenas outside of any pending case or controversy within the meaning of Article III of the U.S. Constitution renders them void and unenforceable.[10] The D.C. Circuit's judgment vacating the district court's orders could be affirmed on the alternative ground that, regardless of the scope of Section 512(h), Congress cannot authorize an Article III court to issue or enforce binding legal process outside of a pending case or controversy. This independent ground for affirmance further counsels in favor of denying certiorari in this case.[11]

---

10. The D.C. Circuit took no position on whether the district court had jurisdiction under Article III to *issue* the subpoenas and instead exercised its jurisdiction over the district court's orders enforcing those subpoenas. Pet. 2a n.1; *see Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83 (1998).

11. Because Verizon does not seek to alter the D.C. Circuit's judgment, Verizon respectfully submits that its Article III arguments (Cont'd)

As interpreted and applied by the district court, Section 512(h) allows for the issuance of a subpoena *duces tecum* on an *ex parte* basis in the absence of a pending case or controversy. The subpoena is then subject to enforcement by an Article III court—without any lawsuit ever being filed (or even promised) and without any attempt to invoke the subject matter jurisdiction of the federal courts to resolve any issue of federal law. Judicial officers are thus engaged in purely investigative duties that are constitutionally reserved to grand juries or administrative agencies. From the Framers' time to the present, this Court consistently has held that Article III forbids the use of the federal courts as free floating investigative bodies to discover facts unconnected to the adjudication of actual cases or controversies.[12]

In *Morton Salt*, this Court made clear that "[t]he *judicial* subpoena power not only is subject to specific constitutional limitations . . . but also is subject to those *limitations inherent in the body that issues them* because of the provisions of the Judiciary Article of the Constitution." 338 U.S. at 642 (emphases added). The Court reaffirmed this principle in *Catholic Conference*, holding that "if a district court does not have subject-matter jurisdiction over the underlying action, and the *process was not issued* in aid of

---

(Cont'd)
are properly before the Court as an alternative ground for affirmance. *Bennett v. Spear*, 520 U.S. 154, 166-67 (1997). Out of an abundance of caution, Verizon has also filed a conditional cross-petition squarely placing the Article III issue before the Court.

12. *E.g.*, *Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 171-72 (1803); *United States v. Ferreira*, 54 U.S. (13 How.) 40 (1851); *Yale Todd's Case*, *printed at* 54 U.S. (13 How.) 52 (1851); *Gordon v. United States*, 117 U.S. Appx. 697, 699-706 (1864); *Muskrat v. United States*, 219 U.S. 346, 353-63 (1911); *United States v. Morton Salt*, 338 U.S. 632, 641-42 (1950); *United States Catholic Conf. v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988); *Hoffmann-La Roche Inc. v. Sperling*, 493 U.S. 165, 174 (1989).

determining that jurisdiction, then the process is void and an order of civil contempt based on refusal to honor it must be reversed." 487 U.S. at 76 (emphasis added).

The district court recognized that "'[f]ederal judicial power itself extends only to adjudication of cases and controversies and it is natural that its investigative powers should be jealously confined to these ends.'" Pet. 60a. It further recognized that, "at the time of issuance, a § 512(h) subpoena will not necessarily be tethered to a present or even anticipated 'adversary proceeding, involving a real, not a hypothetical, controversy' over providing the name." Pet. 74a n.12. Thus, the district court *conceded that no Article III case or controversy was present when the underlying DMCA subpoenas were issued*, but it nonetheless refused to apply the teachings of *Morton Salt* and *Catholic Conference*.

In order to reach the conclusion that Section 512(h) was constitutional, the lower court endorsed the extraordinary proposition that "the clerk's issuance of a § 512(h) subpoena does not involve either the exercise of judicial power or the exercise by federal judges of Article I or Article II-type investigatory power." Pet. 61a. Based upon its belief that the issuance of a Section 512(h) subpoena is "a quintessentially ministerial duty," *id.*, the district court apparently concluded that it does not involve the exercise of the constitutional power of *any* branch of government.

This transparent attempt to side-step well-established limitations on the judicial power must be rejected. The two subpoenas here were issued *in the name of the district court* and carried with them *on the day of their issuance* the enforcement authority that federal courts derive only from Article III of the Constitution. Under the district court's reasoning, as long as the clerk initiates the process, Article III courts can be pulled into myriad purely investigative duties that are clearly forbidden to them by the Constitution.

Finally, beyond the *per se* violation of the requirements of Article III, legislative cooptation of federal judicial clerks for non-judicial duties raises a host of *additional* separation of powers concerns. The clerks of any federal court, including this one, are inferior officers

of the Judicial Branch. 28 U.S.C. § 956; *see Buckley v. Valeo*, 424 U.S. 1, 126 (1976). The assignment of extra-judicial duties to an inferior judicial officer is, in itself, an intrusion into the powers and organization of the Judicial Branch and would necessarily lead to bizarre consequences. The court could be forced to review the clerk's actions for an abuse of discretion or clear error when those actions are authorized by Article I as opposed to Article III. Moreover, the clerk's office would have to decide whether to give priority to the investigative work assigned to it by Congress over the adjudicative work assigned to it by Article III judges.

The district court itself recognized the concern that subpoenas would divert the resources of inferior judicial officers from the work of the courts, but found that at the time of its ruling "no such barrage of requests has occurred." Pet. 73a. Yet in the time between the district court penning those words and the D.C. Circuit's decision reversing the district court on the merits, the district courts were flooded with approximately 4,000 DMCA subpoena requests, such that a spokesperson for the Administrative Office of the U.S. Courts described one clerk's office as "functioning more like a clearing house, issuing subpoenas for all over the country." *RIAA nearing 1,000 subpoenas against file-sharing suspects*, Pioneer Press (July 18, 2003), at http://www.twincities.com/mld/pioneerpress/business/technology/6335275.htm?1c (visited June 21, 2004). In fact, the DMCA subpoenas were "so prolific that the" district court, "already suffering staff shortages, [was] forced to reassign employees from elsewhere in the clerk's office to help process paperwork." *Id.* For these reasons, the district court clearly erred in its Article III analysis, which provides an alternative ground for this Court to affirm the judgment below and a further reason to deny RIAA's petition.

CONCLUSION

For the foregoing reasons, Verizon respectfully submits that the petition for writ of certiorari should be denied. If this Court grants the petition, it should adopt the counter-questions presented and grant Verizon's conditional cross-petition filed concurrently herewith.

Respectfully submitted.

JOHN THORNE*
SARAH B. DEUTSCH
THOMAS M. DAILEY
LEONARD CHARLES SUCHYTA
VERIZON COMMUNICATIONS INC.
1515 N. Courthouse Road
Fifth Floor
Arlington, Va. 22201
(703) 351-3900

ANDREW G. MCBRIDE
KATHRYN COMERFORD TODD
BRUCE G. JOSEPH
KARYN K. ABLIN
DINEEN PASHOUKOS WASYLIK
WILEY REIN & FIELDING LLP
1776 K Street NW
Washington, D.C. 20006
(202) 719-7000

Attorneys for Respondent

* *Counsel of Record*

June 25, 2004

APPENDIX

APPENDIX A

ARTICLE III OF THE UNITED STATES CONSTITUTION

Section 1.

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

Section 2.

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

In all Cases affecting Ambassadors, other public Ministers and Consuls, and those in which a State shall be Party, the supreme Court shall have original Jurisdiction. In all the other Cases before mentioned, the supreme Court shall have appellate Jurisdiction, both as to Law and Fact, with such Exceptions, and under such Regulations as the Congress shall make.

Appendix A

The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed.

Section 3.

Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court.

The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.

APPENDIX B

FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

APPENDIX C

TITLE I OF THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, AS CODIFIED AT 17 U.S.C. §§ 1201-1205

Chapter 12: Copyright Protection and Management Systems

Section 1201. Circumvention of copyright protection systems

(a) Violations regarding circumvention of technological measures.

- (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B)

of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine –

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that –

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection –

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

Appendix C

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional violations. - (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that –

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Appendix C

(2) As used in this subsection –

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other rights, etc., not affected. - (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

Appendix C

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for nonprofit libraries, archives, and educational institutions. - (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph –

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1) –

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be –

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law enforcement, intelligence, and other government activities. - This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term ''information security'' means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

Appendix C

(f) Reverse engineering. - (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption research. –

(1) Definitions. - For purposes of this subsection –

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if –

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption. - In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include –

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section [17 U.S.C.A. §1 et seq.], including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

Appendix C

(4) Use of technological means for research activities. - Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to –

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report to Congress. - Not later than 1 year after the date of the enactment of this chapter [17 U.S.C.A. §1 et seq.],, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on –

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

Appendix C

(h) Exceptions regarding minors. - In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which –

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of personally identifying information. –

(1) Circumvention permitted. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if –

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

Appendix C

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures. - This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security Testing. –

(1) Definition. - For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

Appendix C

(3) Factors in determining exemption. - In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include –

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing. - Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2),[1] provided such technological means does not otherwise violate section[2] (a)(2).

(k) Certain analog devices and certain technological measures. –

(1) Certain analog devices. –

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any –

---

1. So in original. Probably should be "subsection (a)(2)".

2. So in original. Probably should be "subsection".

Appendix C

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

Appendix C

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in –

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder ''conforms to'' the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

Appendix C

(2) Certain encoding restrictions. - No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying –

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

Appendix C

(3) Inapplicability. - This subsection shall not –

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions. - For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

Appendix C

(C) An analog video cassette recorder ''conforms'' to the automatic gain control copy control technology if it –

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms "VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.

(5) Violations. - Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an ''act of circumvention'' for the purposes of section 1203(c)(3)(A) of this chapter.

Appendix C

Section 1202. Integrity of copyright management information

(a) False Copyright Management Information. - No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement –

(1) provide copyright management information that is false, or

(2) distribute or import for distribution copyright management information that is false.

(b) Removal or Alteration of Copyright Management Information. - No person shall, without the authority of the copyright owner or the law –

(1) intentionally remove or alter any copyright management information,

(2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or

(3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law,

knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.

(c) Definition. - As used in this section, the term ''copyright management information'' means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:

(1) The title and other information identifying the work, including the information set forth on a notice of copyright.

(2) The name of, and other identifying information about, the author of a work.

(3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.

(4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.

(5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.

(6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.

(d) Law Enforcement, Intelligence, and Other Government Activities. - This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term ''information security'' means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(e) Limitations on Liability. –

(1) Analog transmissions. - In the case of an analog transmission, a person who is making transmissions in its capacity as a broadcast station, or as a cable system, or someone who provides programming to such station or system, shall not be liable for a violation of subsection (b) if –

(A) avoiding the activity that constitutes such violation is not technically feasible or would create an undue financial hardship on such person; and

(B) such person did not intend, by engaging in such activity, to induce, enable, facilitate, or conceal infringement of a right under this title.

(2) Digital transmissions. –

(A) If a digital transmission standard for the placement of copyright management information for a category of works is set in a voluntary, consensus standard-setting process involving a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to the particular copyright management information addressed by such standard if –

(i) the placement of such information by someone other than such person is not in accordance with such standard; and

(ii) the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title.

(B) Until a digital transmission standard has been set pursuant to subparagraph (A) with respect to the placement of copyright management information for a category of works, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to such copyright management information, if the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title, and if –

(i) the transmission of such information by such person would result in a perceptible visual or aural degradation of the digital signal; or

(ii) the transmission of such information by such person would conflict with –

(I) an applicable government regulation relating to transmission of information in a digital signal;

(II) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted by a voluntary consensus standards body prior to the effective date of this chapter; or

(III) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted in a voluntary, consensus standards-setting process open to participation by a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems.

(3) Definitions. - As used in this subsection –

(A) the term ''broadcast station'' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

(B) the term ''cable system'' has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

Appendix C

Section 1203. Civil remedies

(a) Civil Actions. - Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.

(b) Powers of the Court. - In an action brought under subsection (a), the court –

(1) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution;

(2) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;

(3) may award damages under subsection (c);

(4) in its discretion may allow the recovery of costs by or against any party other than the United States or an officer thereof;

(5) in its discretion may award reasonable attorney's fees to the prevailing party; and

(6) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction

of any device or product involved in the violation that is in the custody or control of the violator or has been impounded under paragraph (2).

(c) Award of Damages. –

(1) In general. - Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either –

(A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or

(B) statutory damages, as provided in paragraph (3).

(2) Actual damages. - The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.

(3) Statutory damages. - (A) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.

(B) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1202 in the sum of not less than $2,500 or more than $25,000.

Appendix C

(4) Repeated violations. - In any case in which the injured party sustains the burden of proving, and the court finds, that a person has violated section 1201 or 1202 within 3 years after a final judgment was entered against the person for another such violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.

(5) Innocent violations. –

(A) In general. - The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.

(B) Nonprofit library, archives, educational institutions, or public broadcasting entities. –

(i) Definition. - In this subparagraph, the term "public broadcasting entity" has the meaning given such term under section 118(g).

(ii) In general. - In the case of a nonprofit library, archives, educational institution, or public broadcasting entity, the court shall remit damages in any case in which the library, archives, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archives, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.

Appendix C

Section 1204. Criminal offenses and penalties

(a) In General. - Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain –

(1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and

(2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.

(b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity. - Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(g).

(c) Statute of Limitations. - No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.

Appendix C

Section 1205. Savings clause

Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the Internet.

APPENDIX D

TITLE II OF THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, AS CODIFIED AT 17 U.S.C. § 512

Section 512. Limitations on liability relating to material online

(a) Transitory digital network communications. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no

such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System caching. –

(1) Limitation on liability. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

Appendix D

(2) Conditions. - The conditions referred to in paragraph (1) are that –

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if –

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information residing on systems or networks at direction of Users. –

(1) In general. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider –

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

Appendix D

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent. - The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification. –

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

Appendix D

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Appendix D

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information location tools. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider –

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on liability of nonprofit educational institutions. - (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if –

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online

access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations. - Any person who knowingly materially misrepresents under this section –

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service

provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of removed or disabled material and limitation on other liability. –

(1) No liability for taking down generally. - Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception. - Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider –

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of

the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification. - To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the

jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability. - A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer. –

(1) Request. - A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request. - The request may be made by filing with the clerk –

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of

an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena. - The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena. - If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena. - Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena. - Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions

of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for eligibility. –

(1) Accommodation of technology. - The limitations on liability established by this section shall apply to a service provider only if the service provider –

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition. - As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and –

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions. - The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief. - (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations. - The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider –

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders. - Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions. –

(1) Service provider. - (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

Appendix D

(2) Monetary relief. - As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(l) Other defenses not affected. - The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of privacy. - Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on –

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction. - Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

(5)

Supreme Court, U.S.
FILED
AUG 30 2004
OFFICE OF THE CLERK

No. 03-1579

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,
Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,
Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the District of Columbia Circuit

REPLY BRIEF

STANLEY PIERRE - LOUIS
LINDA J. ZIRKELBACH
RECORDING INDUSTRY
ASSOCIATION OF AMERICA, INC.
1330 CONNECTICUT AVENUE, NW
Suite 300
Washington, D.C. 20036
(202) 775-0101

DONALD B. VERRILLI, JR.
Counsel of Record
THOMAS J. PERRELLI
JARED O. FREEDMAN
JAMES A. TRILLING
JENNER & BLOCK LLP
601 Thirteenth Street, N.W.
Washington, D.C. 20005
(202) 639-6000

Counsel for Petitioner

August 30, 2004

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20001

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

I. THE EXCEPTIONAL IMPORTANCE OF THE QUESTION PRESENTED JUSTIFIES REVIEW. 1

II. THE D.C. CIRCUIT WAS WRONG. 5

III. SECTION 512(h) IS CONSTITUTIONAL. 9

CONCLUSION 10

TABLE OF AUTHORITIES

CASES

In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) 2

Albertson's Inc. v. Kirkingburg, 527 U.S. 551 (1999) 2

Bonneville International Corp. v. Peters, 347 F.3d 485 (3d Cir. 2003) 1

FCC v. NextWave Personal Communications Inc., 537 U.S. 293 (2003) 3

Morris v. Business Concepts, Inc., 283 F.3d 502 (2d Cir. 2002) 1

Morton v. Ruiz, 415 U.S. 199 (1974) 2

Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186 (1946) 10

Skidmore v. Swift & Co., 323 U.S. 134 (1944) 1

Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984) 3

Thornburg v. Gingles, 478 U.S. 30 (1986) 5

United States v. Mead Corp., 533 U.S. 218 (2001) 1

University of Pennsylvania v. EEOC, 493 U.S. 182 (1990) 10

Whitman v. American Trucking Ass'ns, 531 U.S. 457 (2001) 6

Virginia v. Hicks, 539 U.S. 113 (2003) 10

STATUTES AND RULES

17 U.S.C. § 512(a) 8

17 U.S.C. § 512(c)(1) 6, 7

17 U.S.C. § 512(c)(3)(A) 5, 6, 7

17 U.S.C. § 512(h) ..... *passim*

17 U.S.C. § 512(h)(3) 3

17 U.S.C. § 512(h)(4) 3

17 U.S.C. § 512(h)(5) 3, 6

17 U.S.C. § 512(i) 7

17 U.S.C. § 512(i)(1) 7

17 U.S.C. § 512(j)(1)(B) 9

S. Ct. R. 10(c) 1

LEGISLATIVE MATERIALS

H.R. Rep. No. 105-551(II) (1998) 4

Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (Sept. 16-17, 1997) 8

The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (Sept. 11, 1997) 8

PETITIONER'S REPLY MEMORANDUM

I. THE EXCEPTIONAL IMPORTANCE OF THE QUESTION PRESENTED JUSTIFIES REVIEW.

Verizon's brief in opposition misses the point. Chiding the Recording Industry Association of America ("RIAA") for failing to identify a circuit conflict, Verizon urges "continuation of the normal process whereby multiple circuits are encouraged to address a novel legal issue before any intervention by this Court." Opp. at 14. RIAA does not, however, seek review based on a circuit conflict. The petition identifies a federal statutory issue of "exceptional importance" that should be decided by this Court without delay. *See* Pet. at 2, 15-20, 27-29; *see generally* S. Ct. R. 10(c). With respect to the arguments actually advanced in the petition, Verizon has little to say.

First, Verizon all but ignores the fact that the D.C. Circuit's decision conflicts with the interpretation of § 512(h) adopted by the Copyright Office (the views of which warrant deference[1]) and the United States (which is advocating that interpretation in multiple fora). As the United States has explained, the D.C. Circuit's interpretation "fatally compromises" private copyright enforcement against Internet infringers.[2]

The United States has taken this position because the decision below threatens critical *public* interests in fostering expression, and in the protection of the intellectual property

---

[1] Verizon is incorrect that the Copyright Office's views are "not entitled to any weight in this Court." Opp. at 25. Although *Chevron* deference may not be appropriate, the Office receives *Skidmore* deference. *E.g.*, *Bonneville Int'l Corp. v. Peters*, 347 F.3d 485, 490 (3d Cir. 2003); *Morris v. Business Concepts, Inc.*, 283 F.3d 502, 505-06 (2d Cir. 2002); *see generally Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944); *United States v. Mead Corp.*, 533 U.S. 218, 234-35 (2001).

[2] Br. for United States, *RIAA v. Charter Communications, Inc.*, No. 03-3802, at 16 (8th Cir. filed Feb. 24, 2004).

rights vital to a substantial sector of this nation's economy. The United States' interest in litigating the meaning of § 512(h) distinguishes this case from a garden-variety dispute affecting only private interests. In this respect, this case is like one in which a court of appeals has invalidated a statutory interpretation on which a federal agency has premised its enforcement efforts, a situation in which the Court will grant review absent a circuit conflict. *See, e.g., Albertson's Inc. v. Kirkingburg*, 527 U.S. 551, 562-63 (1999); *Morton v. Ruiz*, 415 U.S. 199, 201-02 (1974).

Second, Verizon has no persuasive response to the point that deferring review would defeat the objectives of § 512. The D.C. Circuit acknowledged that "[t]he stakes are large" here. Pet. App. 16a. Indeed, intellectual property owners are under assault. Every day, millions of ISP subscribers using peer-to-peer ("P2P") technology – "who are ignorant or more commonly disdainful of copyright and in any event discount the likelihood of being sued or prosecuted for copyright infringement," *In re Aimster Copyright Litig.*, 334 F.3d 643, 645 (7th Cir. 2003) (Posner, J.), *cert. denied*, 124 S. Ct. 1069 (2004) – continue to make billions of copyrighted works available for unlawful copying. This piracy drains billions of dollars annually from the companies that produce and disseminate copyrighted works and from the artists who create those works. *See* Brief Amicus Curiae of Motion Picture Ass'n of America, *et al.*, at 5-9.

Yet, at the very moment the threat of massive piracy has become a devastating reality, the D.C. Circuit stripped from copyright owners the most important weapon Congress gave them: the ability to respond quickly. As the Copyright Office has explained, "[i]t is common sense that in order to be able to take action against" Internet infringers, copyright owners must learn their identities. Pet. App. 141a. Only an ISP can provide that information, and § 512(h) provides a means for copyright owners to obtain it promptly. The provision requires district court clerks to "expeditiously

issue" subpoenas upon proper requests from copyright owners, § 512(h)(4), requires that such subpoenas "order the service provider . . . to expeditiously disclose" subscriber identities, § 512(h)(3), and requires ISPs to respond "expeditiously" upon receiving a subpoena, § 512(h)(5). By eliminating the possibility of a rapid response to infringement over P2P networks, the D.C. Circuit has blown a huge hole in § 512's protective structure.

The timing of this Court's review should reflect that reality. Where, as here, a court of appeals decides a novel question of statutory interpretation in a way that has drastic consequences for an important sector of the economy (as well as for important public interests), the Court has not hesitated to grant review without a circuit conflict. *E.g.*, *FCC v. NextWave Personal Communications Inc.*, 537 U.S. 293 (2003); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). Here, the case for immediate review is even stronger because the ongoing infringement constitutes irreparable harm to copyright owners as a matter of law.

Third, Verizon cannot identify any offsetting benefit that justifies delaying review. Verizon does not dispute that the case involves a pure question of statutory interpretation, that the question presented here will recur frequently, or that the factual situation in which it arises is typical. Thus, this case is an ideal vehicle for resolving the issue.

Finally, it is no answer to say that John Doe lawsuits can protect copyright owners while the "normal process" of litigation proceeds. To the contrary, the inefficacy of pre-existing mechanisms, such as John Doe lawsuits, was the very problem Congress enacted § 512(h) to address. A plaintiff in a John Doe suit has no immediate right to third-party discovery to identify a defendant. Rather, a plaintiff must move for permission, and even conscientious district courts can take weeks to rule on such motions. During that time, millions of additional unlawful copies of a copyrighted

song, movie or software can be made and distributed. It is also quite possible that the ISP will have purged its files of information needed to identify an infringing subscriber (ISPs typically retain such information only for limited periods), making judicial relief impossible.

Moreover, a plethora of John Doe lawsuits drains judicial resources, requiring judges to rule on motions for expedited third-party discovery in hundreds of cases and spawning collateral litigation over the propriety and scope of such discovery. In contrast, § 512(h) avoids such burdens by authorizing court clerks rather than judges to issue pre-litigation subpoenas and limiting the scope of discovery to the identities of infringers. *See* H.R. Rep. No. 105-551(II), at 61 (1998) ("The issuing of the order should be a ministerial function performed quickly for this provision to have its intended effect."). The John Doe approach also eliminates the possibility of pre-litigation settlement between the copyright owner and the infringing ISP subscriber, exacerbating the strain on judicial resources.

The availability of John Doe lawsuits thus provides no basis for delaying review. To the contrary, Verizon's endorsement of such suits highlights the bankruptcy of its substantive arguments. Verizon concedes that disclosure of subscriber identities is permitted in John Doe lawsuits (indeed, its argument depends on that concession, for John Doe suits would be futile without third party discovery of the identities of infringing subscribers). The question is thus not *whether* such disclosure will occur but *how* it will occur: through the streamlined § 512(h) process or through the cumbersome John Doe process. The Congress that enacted § 512 surely intended the former.

Nor is the limited geographic reach of the D.C. Circuit's decision a reason to defer review. Although the ruling technically forecloses subpoena enforcement only in the District of Columbia, its practical effect has been to shut

down the use of § 512(h) nationwide against infringement occurring on P2P systems. Before this case, ISPs consistently responded to § 512(h) subpoenas. Pet. at 10. Now ISPs consistently refuse to do so, invoking the D.C. Circuit's decision and turning every subpoena request into a "test case." The prospect of lengthy test cases in other jurisdictions is cold comfort to copyright owners who continue to suffer massive harm.

In view of these considerations, and because there are strong reasons for concluding that the D.C. Circuit misinterpreted § 512(h) (*see* Pet. at 19-27 and Point II *infra*), this Court should grant review now.

II. THE D.C. CIRCUIT WAS WRONG.

There is no merit to Verizon's contention that the D.C. Circuit's interpretation of § 512(h) was "compelled" by settled "canons of statutory construction." Opp. at 19. Indeed, the opposite is true. The D.C. Circuit gave no weight to the plain text of § 512(h), which expressly applies to all "service providers," including those providing solely conduit functions. Pet. at 20. The D.C. Circuit likewise refused to give the language of § 512(c)(3)(A)'s notification provision its ordinary meaning when the court held that, as a matter of law, an ISP could not "disable access" to infringing material on a subscriber's computer, even though as a matter of plain English an ISP can do so by terminating the subscriber's account. Pet. at 22, 23 n.16. Most fundamentally, the D.C. Circuit made no effort to construe § 512(h) in light of the statute's manifest purposes, Pet. at 23, thereby upending "the balance Congress struck" in this "compromise legislation." *See Thornburg v. Gingles*, 478 U.S. 30, 84 (1986). Had the D.C. Circuit adhered to the normal rules of statutory interpretation, it would have agreed with the district court that § 512(h) applies to all ISP functions.

As demonstrated in the Petition at pp. 19-27, the D.C. Circuit erred in concluding that § 512(h)'s cross-reference to

§ 512(c)(3)(A) was intended to limit an ISP's duty to respond to a subpoena to situations in which an ISP also has a duty to "take down" infringing material on its network. Section 512(c)(3)(A) is a notification device. Congress used it in § 512(h) to establish the bona fides of the copyright owner's claim of infringement and to provide the ISP with the information needed to respond to the subpoena. Read this way, the cross-reference to § 512(c)(3)(A) has content, and is obviously not "congressional gibberish." *See* Opp. at 20. There is simply no reason to infer from the cross-reference that Congress implicitly intended to exempt conduit ISPs from § 512(h), a step Congress could easily have taken directly. *See Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001) ("Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions – it does not, one might say, hide elephants in mouseholes.").

Verizon's contrary reading of the statute proceeds from the false premise that § 512(h) "incorporates the subsection (c)(3) 'notice *and take down* procedure' at every stage." Opp. at 6. (emphasis added). In truth, § 512(h) incorporates only the notification requirement, not the "take down" requirement – which is set forth in a different provision, § 512(c)(1), that § 512(h) does not cross-reference. By its terms, therefore, the statute does not require an ISP to "take down" material identified in a notification accompanying a § 512(h) subpoena. The "take down" obligation arises independently under § 512(c)(1), and is triggered or not depending on whether all the requirements of § 512(c) are met (including the requirement in § 512(c)(1) that the infringing material be stored on the ISP's network). A notification can thus satisfy the statute for purposes of § 512(h) even if it does not also trigger the "take down" duty of § 512(c)(1). Congress stated this plainly in § 512(h)(5), which obligates an ISP to respond to a subpoena even where

it does not believe it has any duty to "take down" material pursuant to § 512(c)(1).

Verizon thus misleads when it repeatedly asserts that applying § 512(h) to all ISP functions would require ISPs to terminate the accounts of subscribers who store infringing material on their home computers. An ISP's duty to "take down" infringing material is dictated by other provisions of § 512 – not § 512(h) or § 512(c)(3)(A) – and is not altered one iota by a notification and subpoena served pursuant to § 512(h). Thus, there is no basis for Verizon's contention that applying § 512(h) to all ISP functions is inconsistent with congressional intent because it would result in the termination of subscribers' accounts rather than merely the "taking down" of infringing material. Section 512(h) requires an ISP to provide information to the copyright owner, not to take any other action with respect to the infringing material or the infringing subscriber.

More generally, Verizon mischaracterizes the overall structure of § 512 when it claims that "the particular functions service providers are performing drive the application of *all* the service provider duties contained in § 512]," and must therefore dictate the scope of § 512(h) as well. Opp. at 6 (emphasis added). The duties set forth in § 512(i) – which require ISPs to (i) maintain and enforce a policy of terminating subscribers who are repeat infringers, and (ii) refrain from interfering with standard technical measures copyright owners use to protect against digital piracy, § 512(i)(1), apply to *all* ISPs, irrespective of what functions they provide. Making § 512(h) applicable to ISPs providing all functions is thus not the least bit anomalous.

Finally, Verizon fails to rehabilitate the D.C. Circuit's insupportable assertion that "the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works," Pet. App. 14a – a claim the D.C. Circuit

made to justify its suggestion that Congress should solve the problem the decision below created. In reality, Congress enacted § 512 in response to that very risk. P2P software merely provides a more efficient method of doing what BBS software, FTP sites, and e-mail had already made possible long before the DMCA's passage in 1998 – transferring material from one home computer to another without storing it on an ISP's network. That problem was a focus of the legislative process preceding the DMCA's enactment, and the legislative history discusses the risks posed by BBS, FTP and e-mail dissemination of copyrighted works. *See* Pet. at 2-9. Congress cannot plausibly be thought to have ignored this risk in the DMCA, a statute intended to address digital piracy in a comprehensive and enduring manner.[3]

Nor can Verizon explain why a Congress ignorant of the risk of ISP subscribers directly exchanging files containing copyrighted works would have gone to the trouble of enacting statutory provisions that limit the liability of ISPs providing solely conduit functions, § 512(a), and that authorize injunctive relief requiring ISPs providing conduit

---

[3] Verizon chides RIAA for citing legislative history from "legislation *other than the DMCA*," Opp. at 24 & n.7 (emphasis in original), but that contention is incorrect. The legislative history to which Verizon referred derived from hearings on the "Online Copyright Liability Limitation Act," the original name of the DMCA, Pet. at 5-7, as well as from a series of hearings held on copyright piracy during a single week in September of 1997, when Congress was considering multiple pieces of legislation, including the DMCA. *See Online Copyright Liability Limitation Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (Sept. 16-17, 1997); *Copyright Piracy, and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (Sept. 11, 1997). Indeed, the NET Act, discussed in conjunction with the DMCA, was targeted at infringers who used personal computers to disseminate copyrights works over the Internet without charging for them. Sept. 11, 1997 Hearing at 2 (statement of Chairman Coble) (citing *LaMacchia* case involving an MIT student using a personal computer and FTP software to disseminate copyrighted works).

functions to terminate the accounts of subscribers who directly exchange infringing material without storing it on an ISP's network, § 512(j)(1)(B). The reality is that Congress enacted these provisions precisely because it understood that "internet users might be able directly to exchange files containing copyrighted works." Pet. App. 14a.

Indeed, § 512(j)'s authorization of such injunctive relief is a powerful indicator that Congress intended § 512(h) to cover all ISP functions. A copyright owner could not bring a lawsuit to obtain the injunctive relief authorized by § 512(j)(1)(B) without first ascertaining the identity of the subscriber transmitting infringing material over an ISP's network. Yet only the subscriber's ISP can provide that information. To accept the D.C. Circuit's reading of § 512, therefore, one would have to assume that Congress gave with one hand and took away with the other – *i.e.*, that Congress authorized injunctive relief requiring ISPs to terminate subscribers' accounts even when the ISP has provided only conduit functions, and at the same time denied copyright owners streamlined procedures to obtain the information they need to pursue claims for such injunctive relief. That reading makes no sense.

III. SECTION 512(h) IS CONSTITUTIONAL.

Verizon's constitutional attacks on § 512(h) provide neither a "constitutional avoidance" justification for the D.C. Circuit's decision nor a meritorious alternative ground for affirmance. The doctrine of constitutional avoidance has no principled application here because the alleged infirmities Verizon identifies would apply to the D.C. Circuit's truncated interpretation of § 512(h) just as fully as they would to the interpretation of § 512(h) advanced by petitioners.

In any event, Verizon's constitutional arguments are meritless. RIAA discusses the errors in Verizon's Article III argument in its response to Verizon's conditional cross-

petition. With respect to the First Amendment argument, it suffices to point out that Verizon does not claim its First Amendment rights, or those of the subscribers whose identities RIAA sought, have been infringed. Nor could such a claim be made. Section 512(h) does not forbid, restrain or otherwise abridge any speech. Verizon's First Amendment challenge instead rests on speculation that subscribers other than those whose identities are at issue might refrain from speaking anonymously on the Internet for fear of being wrongly accused of infringement and identified pursuant to § 512(h). That is an overbreadth claim, and Verizon cannot come close to meeting the heavy burden of demonstrating that § 512(h) should be subject to the drastic remedy of facial invalidation – particularly given the procedural protections built into the statute. *See Virginia v. Hicks*, 539 U.S. 113, 123-24 (2003). Moreover, as this Court has repeatedly held, an assertion of First Amendment interests does not limit the enforcement of legal process. *See Univ. of Pa. v. EEOC*, 493 U.S. 182, 199-200 (1990); *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 192-93 (1946).

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

STANLEY PIERRE-LOUIS
LINDA J. ZIRKELBACH
RECORDING INDUSTRY
ASSOCIATION OF AMERICA, INC.
1330 Connecticut Avenue, NW
Suite 300
Washington, D.C. 20036
(202) 775-0101

DONALD B. VERRILLI, JR.
Counsel of Record
THOMAS J. PERRELLI
JARED O. FREEDMAN
JAMES A. TRILLING
JENNER & BLOCK LLP
601 Thirteenth Street, NW
Washington, D.C. 20005
(202) 639-6000

Counsel for Petitioner

August 30, 2004

(2)

No. 03-1579

Supreme Court, U.S.
FILED
JUN 25 2004
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,
Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the District of Columbia Circuit

BRIEF *AMICI CURIAE* OF MOTION PICTURE ASSOCIATION OF AMERICA, INC., CHURCH MUSIC PUBLISHERS ASSOCIATION, ASSOCIATION OF AMERICAN PUBLISHERS, INC., AFMA, ENTERTAINMENT SOFTWARE ASSOCIATION, SCREEN ACTORS GUILD, INC., DIRECTORS GUILD OF AMERICA, INC., PRODUCERS GUILD OF AMERICA, INC., WRITERS GUILD OF AMERICA, WEST, INC., THE AUTHORS GUILD, RECORDING ARTISTS COALITION, SOFTWARE & INFORMATION INDUSTRY ASSOCATION, SESAC, INC., THE SONGWRITERS GUILD OF AMERICA, PROFESSIONAL PHOTOGRAPHERS OF AMERICA, AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS, BROADCAST MUSIC, INC., AMERICAN FEDERATION OF MUSICIANS, GRAPHIC ARTISTS GUILD, INC., NASHVILLE SONGWRITERS ASSOCIATION INTERNATIONAL, AND AMERICAN SOCIETY OF MEDIA PHOTOGRAPHERS, INC., IN SUPPORT OF PETITION FOR CERTIORARI

STEVEN J. METALITZ
ERIC J. SCHWARTZ
SMITH & METALITZ LLP
1747 Pennsylvania Avenue, N.W.
Suite 825
Washington, D.C. 20006
(202) 833-4198
Attorneys for Other Amici Curiae

JOHN G. KESTER *
PAUL B. GAFFNEY
JOSEPH M. TERRY
WILLIAMS & CONNOLLY LLP
725 12th Street, N.W.
Washington, D.C. 20005
(202) 434-5069
Attorneys for Amicus Curiae Motion Picture Association of America, Inc.

* Counsel of Record

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20001

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	iii
INTEREST OF THE *AMICI CURIAE*	1
SUMMARY OF ARGUMENT	2
ARGUMENT	3
I. INTERNET COPYRIGHT PIRACY THREATENS THE CREATIVE INDUSTRIES AND UNDERMINES THE RULE OF LAW.	3
A Stealing Music, Movies and Other Copyrighted Works Has Become "Epidemic."	3
B. Stealing Via the Internet Threatens Major Industries and Their Employees.	5
C. The Corrosive Effect of Widespread Internet Theft Is Heightened by the Court of Appeals' Decision	8
II. THE COURT OF APPEALS EVISCERATED CONGRESS'S CAREFULLY CONSIDERED REMEDY FOR INTERNET PIRACY.	9
A. The Court of Appeals Undid the Legislative Bargain.	9
B. Congress Was Well Aware of and Intended To Address New Piracy Technologies.	12
III. THE COURT OF APPEALS' DECISION DESTROYS THE EFFECTIVE ENFORCEMENT THE STATUTE INTENDED.	14
IV. THE URGENCY AND IMPORTANCE OF THIS CRIME WAVE CALL FOR CERTIORARI NOW	17

TABLE OF CONTENTS—Continued

	Page
A. Entire Industries Are Threatened.....	17
B. The Court of Appeals' Decision Rejects the Interpretation of the Statute by the Copyright Office.....	18
C. The Court of Appeals' Decision Rejects the Interpretation of the Statute by the United States.....	19
D. There Is No Reason for Delay.....	20
CONCLUSION	20

TABLE OF AUTHORITIES

Cases: Page

A & M Records, Inc. v. *Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001) 5, 16

In re Aimster Copyright Litig., 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) 3, 5

In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) 8, 16

Almendarez-Torres v. *United States*, 523 U.S. 224 (1998) 15

Barnhart v. *Sigmon Coal Co.*, 534 U.S. 438 (2002) 12

BMG Music et al. v. *Does 1-203*, No. 04-650 (E.D. Pa. Mar. 5, 2004) 16

Brotherhood of R.R. Trainmen v. *Baltimore & O.R.R.*, 331 U.S. 519 (1947) 15

Commissioner v. *Lincoln Savings & Loan Ass'n*, 403 U.S. 345 (1971) 18

De Sylva v. *Ballentine*, 351 U.S. 570 (1956) 17

Fortnightly Corp. v. *United Artists Television, Inc.*, 392 U.S. 390 (1968) 14, 17

Haggar Co. v. *Helvering*, 308 U.S. 389 (1940) 15

Harper & Row, Publishers, Inc. v. *Nation Enterprises*, 471 U.S. 539 (1985) 7

INS v. *National Center for Immigrants' Rights, Inc.*, 502 U.S. 183 (1991) 15

Interscope Records v. *Does 1-25*, No. 6:04-CV-197-ORL-22-DAB (M.D. Fla. Apr. 27, 2004) .. 16

Jerome H. Remick & Co. v. *American Automobile Accessories Co.*, 5 F.2d 411 (6th Cir.), *cert. denied*, 269 U.S. 556 (1925) 14

TABLE OF AUTHORITIES—Continued

	Page
Linn v. *United Plant Guard Workers*, 383 U.S. 53 (1966)	8
Metro-Goldwyn-Mayer Studios, Inc. v. *Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *appeal pending*, No. 03-55894 (9th Cir., argued Feb. 3, 2004)	5, 16
Mills Music, Inc. v. *Snyder*, 469 U.S. 153 (1985)	17
Mohasco Corp. v. *Silver*, 447 U.S. 807 (1980)	11
National Broiler Marketing Ass'n v. *United States*, 436 U.S. 816 (1978)	18
Ragsdale v. *Wolverine World Wide, Inc.*, 535 U.S. 81 (2002)	11
Recording Industry Ass'n v. *Charter Communications, Inc.*, No. 03-3802 (8th Cir., argued June 14, 2004)	19
Robert C. Herd & Co. v. *Krawill Machinery Corp.*, 359 U.S. 297 (1959)	18
SEC v. *Capital Gains Research Bureau, Inc.*, 375 U.S. 180 (1963)	18
Thornburg v. *Gingles*, 478 U.S. 30 (1986)	11
Twentieth Century Music Corp. v. *Aiken*, 422 U.S. 151 (1975)	7, 14
United States v. *Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002)	3
United States v. *Mitchell*, 463 U.S. 206 (1983)	18
United States v. *Riverside Bayview Homes, Inc.*, 474 U.S. 121 (1985)	19
United States v. *Taylor*, 487 U.S. 326 (1988)	2, 11
United States v. *Zazove*, 334 U.S. 602 (1948)	18
Weinberger v. *Hynson, Westcott & Dunning, Inc.*, 412 U.S. 609 (1973)	15
West v. *Gibson*, 527 U.S. 212 (1999)	14

TABLE OF AUTHORITIES—Continued

Page

Yellow Transp., Inc. v. *Michigan*, 537 U.S. 36 (2002) 19

Constitutional Provisions:

U.S. Const., Art. I, § 8, cl. 8 7

Statutes:

Online Copyright Infringement Liability Limitation Act § 201, 17 U.S.C. § 512 (1998) .....2, *passim*

Rules:

Federal Rules of Civil Procedure, Rule 45 16

Rules of the Supreme Court of the United States, Rule 37 1

Miscellaneous:

J. Bernoff, *et al.*, *From Discs to Downloads* (Aug. 23, 2003), *available at* Forrester Research, http://www.forrester.com 9

Brief for the United States as Intervenor and *Amicus Curiae*, *Recording Industry Ass'n* v. *Charter Communications, Inc.*, No. 03-3802 (8th Cir.) 19

J. Calvert, *PC Gamers Admit to Piracy* (June 11, 2004), *available at* http://www.gamespot.com/news/2004/06/11/news_6100456.html 6

Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1146 Before Senate Comm. on Judiciary, 105th Cong. (1997) 10, 13

TABLE OF AUTHORITIES—Continued

Page

Copyright Piracy and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before Subcomm. on Courts and Intellectual Property, House Comm. on Judiciary, 105th Cong. (1997) 12

Deloitte & Touche, *Facing Piracy* (2004) 3, 4, 6

Graham, *Online Trading of TV Episodes Grows*, USA Today, May 20, 2004, at 3B 3

H.R. Rep. No. 105-551 (1998) 9, 11

Johnson, *Cybervillains*, The Guardian, May 20, 2002, at 40 6

Kirkland, *Criminal Downloading of Movies Off the Internet and Piracy of DVDs Is Shaking the Industry to the Core*, Toronto Sun, April 13, 2004 7

Lowe, *Movie Industry Arms Itself To Sink Pirates*, Sydney Morning Herald, April 14, 2004 4

McGuire, *Internet Piracy*, Washington Post, Jan. 22, 2004 6

Motion Picture Association, Press Release, July 22, 2003 6

NII Copyright Protection Act of 1995 (Part 2): Hearing Before Subcomm. on Courts and Intellectual Property, House Comm. on Judiciary, 104th Cong. (1996) 10

Pew Internet & American Life Project, *Broadband Penetration on the Upswing* (April 2004), *available at* http://www.pewinternet.org/pdfs/PIP_Broadband04.DataMemo.pdf 4

TABLE OF AUTHORITIES—Continued

	Page
Pew Internet & American Life Project, *The State of Music Downloading and File-Sharing Online* (April 2004), *available at* http://www.pewinternet.org/pdfs/PIP_Filesharing_April04.pdf	8
Raymond, *Penumbral Crimes*, 39 AM. CRIM. L. REV. 1395 (2002)	8
S. 2037, 105th Cong. (1998)	10
S. Rep. No. 105-190 (1998)	11
S. Siwek, *Copyright Industries in the U.S. Economy: 2002 Report* (2002)	5
WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and 2280 Before Subcomm. on Courts and Intellectual Property, House Comm. on Judiciary, 105th Cong. (1997)	10
WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before Subcomm. on Telecommunications, Trade and Consumer Protection, House Comm. on Commerce, 105th Cong. (1998)	11, 13

BRIEF *AMICI CURIAE* OF MOTION PICTURE ASSOCIATION OF AMERICA, INC., CHURCH MUSIC PUBLISHERS ASSOCIATION, ASSOCIATION OF AMERICAN PUBLISHERS, INC., AFMA, ENTERTAINMENT SOFTWARE ASSOCIATION, SCREEN ACTORS GUILD, INC., DIRECTORS GUILD OF AMERICA, INC., PRODUCERS GUILD OF AMERICA, INC., WRITERS GUILD OF AMERICA, WEST, INC., THE AUTHORS GUILD, RECORDING ARTISTS COALITION, SOFTWARE & INFORMATION INDUSTRY ASSOCATION, SESAC, INC., THE SONGWRITERS GUILD OF AMERICA, PROFESSIONAL PHOTOGRAPHERS OF AMERICA, AMERICAN FEDERATION OF TELEVISION AND RADIO ARTISTS, BROADCAST MUSIC INC., AMERICAN FEDERATION OF MUSICIANS, GRAPHIC ARTISTS GUILD, INC., NASHVILLE SONGWRITERS ASSOCIATION INTERNATIONAL, AND AMERICAN SOCIETY OF MEDIA PHOTOGRAPHERS, INC., IN SUPPORT OF PETITION FOR CERTIORARI

Pursuant to this Court's Rule 37.1(a), the entities listed above respectfully submit this brief *amici curiae* in support of petitioner. Written consents of both petitioner and respondent to the filing of this brief have been filed with the Clerk.[1]

INTEREST OF THE *AMICI CURIAE*

Amici are a broad coalition of organizations that represent the artists, authors, songwriters, producers, publishers, and distributors of music, films, television, literature, video

---

[1] In accordance with Rule 37.6, no counsel for a party authored this brief in whole or in part and no person other than *amici curiae* or their members made a monetary contribution to the preparation or submission of this brief.

games, photographic art, and computer software. Although diverse in their creative pursuits, *amici* share a common interest: their industries' survival depends on the protection of lawful intellectual property rights in the artistic works that are created, produced, and distributed by their members.

SUMMARY OF ARGUMENT

This is a case of extraordinary importance for the creative industries, for the public, and for the rule of law. The D.C. Circuit acknowledged that "[t]he stakes are large for the music, motion picture, and software industries and their role in fostering technological innovation and our popular culture." Pet. App. 16a. What impends from this decision, contrary to the plain intent of Congress, is a disaster that will undermine not only the music industry, but the motion picture, software and other creative industries, whose companies and workers contribute enormously to the economy and the culture.

The Court of Appeals not only gave the "Subpoena to identify infringer" provision of the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), a tortured interpretation utterly at odds with the express intentions negotiated by the enactors. The Court of Appeals also violated established principles of construction that when, as here, Congress has enacted a compromise to balance competing interests, the resulting statute is not to be judicially dismantled, leaving only half the bargain in place. *United States* v. *Taylor*, 487 U.S. 326, 336 (1988). And the Court of Appeals further violated this Court's years of decisions that hold that copyright protections must not be held negated by technological modifications that enable substantially the same infringement techniques that Congress sought to eliminate.

This decision already is having enormous and deleterious economic effect. The cost is in dollars, jobs, and respect for law. It is an inevitable issue of construction that can be

decided authoritatively only by this Court, and the sooner it is determined, the better.

ARGUMENT

I. INTERNET COPYRIGHT PIRACY THREATENS THE CREATIVE INDUSTRIES AND UNDERMINES THE RULE OF LAW.

A. Stealing Music, Movies and Other Copyrighted Works Has Become "Epidemic."

As the District Court observed, the massive copyright piracy that is the dark side of the Internet "is well-recognized and 'has reached epidemic proportions.'" Pet. App. 92a (quoting *United States* v. *Elcom Ltd.*, 203 F. Supp. 2d 1111, 1132 (N.D. Cal. 2002)); *see also In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 649 (N.D. Ill. 2002) (describing the "ongoing, massive, and unauthorized distribution and copying" of copyrighted works), *aff'd*, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004). Indeed, noted the District Court, piracy of copyrighted music has "skyrocketed." Pet. App. 106a.

Starting later, but rising exponentially year by year, has been the piracy of copyrighted motion pictures, which now is costing billions of dollars. Currently an estimated 400,000 to 600,000 motion pictures are illegally downloaded *every day* in the United States, and almost 20,000 unauthorized digital copies of such popular television shows as "The Simpsons" and "Alias" are unlawfully available for download on the Internet. Deloitte & Touche, *Facing Piracy* 13 (2004); Graham, *Online Trading of TV Episodes Grows*, USA Today, May 20, 2004, at 3B (citing BayTSP report).

The film industry's distress exemplifies what all copyright owners now face. As the number of users, the speed of Internet connections, and the technical capacity of personal computers have continued to increase, so, too, has the piracy. As of March 2004, 68 million adult Americans, or 55% of all

adult Internet users, have access to high-speed Internet connections either at home or at work. Fully 48 million adult Americans have broadband connections at home, an increase of 60% since March 2003. Pew Internet & American Life Project, *Broadband Penetration on the Upswing* 1 (April 2004), *available at* http://www.pewinternet.org/pdfs/PIP_Broadband04.Data Memo.pdf. High-speed Internet connections, new compression technologies, and new file-sharing programs, now let thieves download a perfect digital copy of a full-length motion picture like "The Matrix Reloaded" in about the same time it takes to watch the film. Deloitte & Touche at 13.

With ever-improving technology, the global incidence of illegal downloading of copyrighted filmed entertainment has also increased dramatically. From 2001 to 2003 the number of Internet sites known to be offering pirated motion pictures more than quadrupled—rising from 54,000 to 225,000. Lowe, *Movie Industry Arms Itself To Sink Pirates*, Sydney Morning Herald, April 14, 2004, at 3.

The most prominent and pernicious vehicles of Internet piracy are the peer-to-peer (P2P) "file-sharing" systems and services such as KaZaA and Morpheus—which respondent Verizon, to lure customers to its broadband service, brazenly *recommended to its customers by name!*[2] They serve as nothing more than high-tech piratical bazaars, offering users a staggering array of copyrighted motion pictures (many of which are still in theaters), music, television programming,

---

[2] The marketing material Verizon sent prospective broadband customers stated:

> "[T]he official sites typically don't offer all music that is still selling exceedingly well in stores. *By contrast, the free sites are likely to have pretty much everything* . . . ."

Joint Appendix, Court of Appeals, at 509 (emphasis supplied). Verizon recommended Morpheus by name as an "Essential Site" for "file-sharing fiends." *Id.* at 510.

software and video games. According to one study, nearly 90% of the content offered on such services is copyrighted and distributed without permission from the copyright holder. *See A & M Records, Inc.* v. *Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001). The backers of the KaZaA "file-sharing" system brag that its file-sharing software has been downloaded over 230 million times.

Courts have held without exception or even serious dispute that *individuals who use* these file-copying services to download copyrighted works and make them available to others—the individuals whose identity petitioner seeks to learn in these proceedings—are engaged in direct copyright infringement. *See, e.g., A & M Records*, 239 F.3d at 1114; *Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1034 (C.D. Cal. 2003), *appeal pending*, No. 03-55894 (9th Cir., argued Feb. 3, 2004); *Aimster*, 252 F. Supp. 2d at 652.

B. Stealing Via the Internet Threatens Major Industries and Their Employees.

As the Court of Appeals recognized, "[t]he stakes are large." Pet App. 16a. By 2001, U.S. copyright industries, some of the world's most creative, accounted for 5.24% of the GDP, amounting to $535.1 billion—an increase of over $75 billion from 1999, and for the first time exceeding 5% of the economy. S. Siwek, *Copyright Industries in the U.S. Economy: 2002 Report* 3 (2002). That same year, U.S. copyright industries achieved estimated foreign sales and exports of $88.97 billion, leading all major industry sectors, and contributing substantially and positively to the U.S. balance of payments. *Id.* at 4-5. Between 1977 and 2001, the U.S. copyright industries' share of the GDP grew more than twice as fast as the remainder of the U.S. economy (7% annually compared to 3%). *Id.* at 4. Employment in the copyright industries—including motion pictures, music and software—grew, on average, more than three times faster

(5% annually compared to 1.5%), and more than doubled to 4.7 million workers. The industries threatened by this decision provide 3.5 percent of total U.S. employment. *Id.* at 4. The U.S. motion picture industry alone employs 580,000 people. Motion Picture Association, Press Release, July 22, 2003 (citing U.S. Bureau of Labor Statistics).

Copyright piracy, however, is having an enormous destructive effect. As petitioner points out, the music industry has suffered substantial declines in sales. *See* Pet. 18. Piracy costs the video game industry more than $3 billion per year—a number on the rise as the result of high-speed Internet file-sharing. J. Calvert, *PC Gamers Admit to Piracy* (June 11, 2004), *available at* http://www.gamespot.com/news/2004/06/11/news_6100456.html. Although the music industry has been Internet piracy's leading victim so far, the impending threat is no less serious for the motion picture industry. Feature film and television are the fastest growing media on file-sharing networks. McGuire, *Internet Piracy*, Washington Post, Jan. 22, 2004. According to one independent estimate, the "epidemic," Pet. App. 92a, of Internet piracy already now costs the motion picture industry between $3 to $4 billion *per year* in lost revenue. Deloitte & Touche at 9. Such piracy can strike a motion picture—and harm its commercial success—not only in the DVD market, but even before a work is released. For example:

- In 2002 an estimated one million infringers downloaded "Star Wars: Episode 2—Attack of the Clones" from the Internet a week before it was released in U.S. theaters. Johnson, *Cybervillains*, The Guardian, May 20, 2002, at 40.
- In June 2003 an unauthorized and unfinished copy of the motion picture "The Hulk" appeared on the Internet, several weeks before the film opened in theaters. The stolen copy was an early rough cut containing primitive special effects that were to be replaced by polished visuals for the final version. The

> unfinished copy was widely disseminated throughout the Internet and the film became the target of widespread criticism in online chat rooms even before it was completed or released to the public. Kirkland, *Criminal Downloading of Movies Off the Internet and Piracy of DVDs Is Shaking the Industry to the Core*, Toronto Sun, April 13, 2004, at 48.

These are just examples of the estimated *$13.6 billion* in lost revenues that the creative industries—including music, games, and motion pictures—now suffer each year at the hands of copyright pirates. Deloitte & Touche at 9.

Such pervasive lawlessness threatens not just the direct victims of piracy—the studios, theaters, artists, authors, producers, directors, and countless individuals involved in the creation, distribution and retailing of motion pictures and other creative works—but the public as well. Copyright laws, as contemplated by the Copyright Clause, U.S. Const., Art. I, § 8, cl. 8, motivate authors, composers, and artists to invest their time and efforts in the development of new works, secure in the knowledge that they will maintain exclusive control over, and reap the rewards of, their creative expression. "[T]he ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good." *Twentieth Century Music Corp.* v. *Aiken*, 422 U.S. 151, 156 (1975).

> "[I]t should not be forgotten that the Framers intended copyright itself to be the engine of free expression. By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas."

Harper & Row, Publishers, Inc. v. *Nation Enterprises*, 471 U.S. 539, 558 (1985). But if copyright laws may be flouted, the constitutional and congressional goal is hampered or destroyed.

C. The Corrosive Effect of Widespread Internet Theft Is Heightened by the Court of Appeals' Decision.

The Court of Appeals' neutering of the statute Congress enacted to remedy this catastrophe effectively sanctions one of the greatest outbreaks of lawlessness this country has ever seen. Worse, the greatest number of those who daily steal music, motion pictures, and other copyrighted material via the Internet are young people. The lesson they are being taught is that they may take the property created by the hard work of others, and scoff at the law. It is no different than if they entered a store, helped themselves to a bag full of music CDs, DVDs, software programs and video games, and walked out without paying, and without penalty. As the Seventh Circuit observed:

> "Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. . . . The swappers, who are ignorant or *more commonly disdainful of copyright* and in any event *discount the likelihood of being sued or prosecuted* for copyright infringement, are the direct infringers."

In re Aimster Copyright Litig., 334 F.3d at 645 (Posner, J.) (emphasis supplied). "[T]he refusal to redress an otherwise actionable wrong creates disrespect for the law . . . ." *Linn* v. *United Plant Guard Workers*, 383 U.S. 53, 64 n.6 (1966). "If disobeying the law has no consequences, then disobedience will become more likely." Raymond, *Penumbral Crimes*, 39 AM. CRIM. L. REV. 1395, 1424 (2002).

Congress in the Digital Millennium Copyright Act enacted a method of enforcement to restrain this lawlessness, a method that was beginning to show success.[3] After the Court

---

[3] Six months after the RIAA announced that it would begin filing lawsuits against individual music downloaders, the percentage of Internet users who reported downloading music fell by 50%. *See* Pew Internet & American Life Project, *The State of Music Downloading and File-Sharing*

of Appeals' decision, however, a generation is learning that laws are made to be broken, and penalty is unlikely—indeed, that "everybody does it" and few are caught. Perhaps most disturbingly, according to a survey released last summer by an independent technology research firm, *nearly half* of all 12-to-23-year-olds reported that they had downloaded music the prior month—and half of those said they now buy fewer CDs. One-fifth of those had also downloaded a motion picture. J. Bernoff, *et al.*, *From Discs to Downloads* (Aug. 23, 2003), *available at* Forrester Research, http://www.forrester.com.

II. THE COURT OF APPEALS EVISCERATED CONGRESS'S CAREFULLY CONSIDERED REMEDY FOR INTERNET PIRACY.

A. The Court of Appeals Undid the Legislative Bargain.

The DMCA embodies a carefully balanced negotiated legislative bargain. The Internet service provider ("ISP") industry—which includes respondent—recognized that established copyright law, including contributory and vicarious infringement, exposed ISPs to enormous potential monetary liability for the infringing conduct of their customers. *See* H.R. Rep. No. 105-551 (Amended), pt. 1, at 11 (1998). ISPs asked for broad legislative immunity from damage claims arising from the infringing conduct of their users. But the software, motion picture, video game, and recording industries—the entities that were suffering, and would continue to suffer, the consequences of Internet copyright theft—pointed out that if ISPs were to be granted a free pass

---

Online 6 (April 2004), *available at* http://www.pewinternet.org/pdfs/PIP_Filesharing_ April04.pdf. Fourteen percent of the 128 million American adults now online report that they downloaded music at one time, but now no longer do so. *About one-third of these former music downloaders—6 million adults—say that threat of legal actions are the reason they stopped. Id.* at 1. *See also* Pet. 27 n.18.

from infringement liability, balance and fairness required some complementary provision under which copyright owners could quickly learn the identity of, and assert claims against, the ISP customers suspected of copyright infringement.[4] As early as 1996, at least one prominent member of the ISP community, CompuServe, agreed, and had proposed that, in exchange for immunity, ISPs should become responsible both for taking down infringing works located on their servers when notified of the infringements, and in assisting copyright owners in identifying infringers. *NII Copyright Protection Act of 1995 (Part 2): Hearing Before Subcomm. on Courts and Intellectual Property, House Comm. on Judiciary*, 104th Cong. 261 (1996).

Following a lengthy negotiation process among the interested parties, the Senate in May 1998 passed S. 2037, 105th Cong. Section 202 of S. 2037, which is virtually the same as 17 U.S.C. § 512 as ultimately enacted, includes a provision entitled "Identification of Direct Infringer" that

---

[4] *See Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1146 Before Senate Comm. on Judiciary*, 105th Cong. 45-55 (1997); *WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and 2280 Before Subcomm. on Courts and Intellectual Property, House Comm. on Judiciary*, 105th Cong. 22-25 (1997). As explained by an industry group representing leading software firms:

> "A matter not now addressed by the bill is disclosure of the names and addresses of infringers by the service provider. Often in conducting Internet anti-piracy cases, we can locate the source of the material as a particular site on a service provider's system, but because the Internet is essentially an environment replete with 'aliases,' we cannot determine the identity of a person."

Id. at 77 (Business Software Alliance). Likewise, the Information Industry Association urged Congress to "condition reduced liability for infringement on the access or service provider's willingness to reveal the names of users that violate copyright and to preclude repeat offenders from accessing their services." *Id.* at 177.

BEST AVAILABLE COPY

served the same function as the provision, § 512(h), at issue in this litigation. At House committee hearings, the ISP industry came out "very much in support" of the compromise legislation.[5] The House thereafter accepted the compromise as "preserv[ing] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." H. Rep. No. 105-551, pt. 2, at 49 (1998); *see also* S. Rep. No. 105-190, at 20 (1998) (same). Thus the DMCA, as enacted, was Congress's comprehensive attempt to combat this lawlessness while accommodating in balanced fashion the monetary liability concerns of Internet service providers like respondent. Among the keys of that balance is the section at issue in this case, 17 U.S.C. § 512(h).

In reversing the District Court and holding that Section 512(h) does not protect copyright owners after all against "peer-to-peer" (P2P) Internet piracy, the Court of Appeals cast aside the legislative compromise reflected in Title II of the DMCA. The decision leaves ISPs largely exempt from monetary liability—while stripping copyright owners of their critical half of the bargain Congress had granted them in the battle against online piracy. Such deformation of a carefully wrought negotiated statute this Court repeatedly has condemned. "In construing this compromise legislation, we must make every effort to be faithful to the balance Congress struck." *Thornburg* v. *Gingles*, 478 U.S. 30, 84 (1986). "Courts and agencies must respect and give effect to these sorts of compromises." *Ragsdale* v. *Wolverine World Wide, Inc.*, 535 U.S. 81, 94 (2002). "[R]eview must serve to ensure that the purposes of the Act and the legislative compromise it reflects are given effect." *United States* v. *Taylor*, 487 U.S. 326, 336 (1988). *Accord, e.g.*, *Mohasco Corp.* v. *Silver*, 447

---

[5] *WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before Subcomm. on Telecommunications, Trade and Consumer Protection, House Comm. on Commerce*, 105th Cong. 50-52 (1998).

U.S. 807, 826 (1980) ("We must respect the compromise embodied in the words chosen by Congress"); *Barnhart* v. *Sigmon Coal Co.*, 534 U.S. 438, 461 (2002) ("The deals brokered . . . are not for us to judge or second-guess").

B. Congress Was Well Aware of and Intended To Address New Piracy Technologies.

The Court of Appeals believed that "the legislative history of the DMCA betrays no awareness whatsoever that Internet users might be able directly to exchange files containing copyrighted works." Pet. App. 14a. But that characterization is misleading, because quite demonstrably Congress anticipated technological change. The specific current P2P technology may not have been available; but the history of the DMCA shows that Congress was well aware that the technologies of piracy were constantly evolving, along with the Internet itself, and that it intended to address the problem, not some particular technical means. In treating P2P infringement technology as something utterly new and surprising, and on that basis outside the DMCA, the Court of Appeals was factually and legally far astray.

1. Although Internet copyright piracy had not yet reached the "epidemic proportions," Pet. App. 92a, that exist now, by 1997 Congress already was hearing from numerous witnesses who warned that "[c]opyright owners today lose substantial sums of money to copyright pirates." *Copyright Piracy and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before Subcomm. on Courts and Intellectual Prop., House Comm. on Judiciary*, 105th Cong. 12 (1997) (Register of Copyrights Peters).

> "The advent of digital technology has the potential to exacerbate greatly the impact of piracy. . . . As it becomes easier to transmit large amounts of data quickly over the [Internet] it becomes easier for those without a commercial stake or profit motive—. . . an Internet user

> opposed to copyright law—to inflict tremendous damage to the market for a copyrighted work."

Id. That Internet piracy predictably would manifest itself in constantly new techniques was made clear by other witnesses as well:

> "Although distributing software through [electronic bulletin boards] is the method of choice for present-day computer pirates, other computer network services are providing new means for copyright crime to occur. For example . . . [p]rograms can be sent . . . through World Wide Web sites or other programs that allow for the rapid exchange of digital information."

Id. at 17 (Assistant Attorney General DiGregory).

By 1998 there was no doubt that Internet piracy soon would also attack the motion picture industry, which warned Congress that piracy of its product, although not yet rampant, would inevitably grow along with faster copying technology:

> "Movies and videos are not much in evidence yet. That is because the audio-visual content is so rich in information that it cannot yet move easily through the digital network. The volume of flow is simply too great for some of the pipes. But we also know that our present reprieve is only temporary. The same technology that will smooth the way for legitimate delivery of video on demand over digital networks will also prime the pump for copyright pirates."

Hearing on S. 1146, at 8-9 (MPAA Senior Vice President Attaway). The head of the Business Software Alliance likewise warned that "[p]iracy of software is a major and growing problem," and warned that the Internet could "become a haven for thieves." *Hearing on H.R. 2281*, at 37-40.

2. The Court of Appeals' reasoning is, as the United States points out along with petitioner, "palpably wrong" not only for the basic reasons of textual construction set forth in the Petition. *See* Pet. 21. The Court of Appeals also ignored, and violated,

admonitions about construing copyright legislation that this Court has reiterated for years. When applying copyright legislation even to changes in technology far more sweeping than those here, this Court explained that "[w]e must read the statutory language of 60 years ago in the light of drastic technological change." *Fortnightly Corp.* v. *United Artists Television, Inc.*, 392 U.S. 390, 396 (1968). "When technological change has rendered its literal terms ambiguous, the Copyright Act must be construed in light of [its] basic purpose." *Twentieth Century Music Corp.* v. *Aiken*, 422 U.S. 151, 156 (1975). *See also West* v. *Gibson*, 527 U.S. 212, 218 (1999) ("Words in statutes can enlarge or contract their scope as other changes, in law or in the world, require their application to new instances or make old applications anachronistic.")

> "While statutes should not be stretched to apply to new situations not fairly within their scope, they should not be so narrowly construed as to permit their evasion because of changing habits due to new inventions and discoveries."

Fortnightly Corp., 392 U.S. at 395 n.16 (quoting *Jerome H. Remick & Co.* v. *American Automobile Accessories Co.*, 5 F.2d 411 (6th Cir.), *cert. denied*, 269 U.S. 556 (1925)).

III. THE COURT OF APPEALS' DECISION DESTROYS THE EFFECTIVE ENFORCEMENT THE STATUTE INTENDED.

The Court of Appeals' decision disables the statute. By the holding that 512(h) subpoenas may be issued only in cases where an infringer has posted infringing works on a service provider's Internet server, copyright owners have been robbed of the very remedy the statute was enacted to afford them, crippling their ability to combat what is now the most virulent and widespread form of online copyright infringement. As the District Court recognized:

> "There is little doubt that the largest opportunity for copyright theft is through peer-to-peer ('P2P') software, as used by the alleged infringer here. . . . Thus, under

> Verizon's reading of the Act, a significant amount of potential copyright infringement would be shielded from the subpoena authority of the DMCA. That would, in effect, give Internet copyright infringers shelter from the long arm of the DMCA subpoena power, and allow infringement to flourish."

Pet. App. 37a.

The Court of Appeals throughout ignored the fundamental canon of statutory construction that "[a]ll statutes must be construed in the light of their purpose. A literal reading of them which would lead to absurd results is to be avoided when they can be given a reasonable application consistent with their words and with the legislative purpose." *Haggar Co.* v. *Helvering*, 308 U.S. 389, 394 (1940); *see also Weinberger* v. *Hynson, Westcott & Dunning, Inc.*, 412 U.S. 609, 631-32 (1973) ("It is well established that our task in interpreting separate provisions of a single Act is to give the Act the most harmonious comprehensive meaning possible in light of the legislative policy and purpose.").

The Court of Appeals also paid no heed to the caption Congress placed on § 512(h): "Subpoena to identify infringer." "'[T]he title of a statute and the heading of a section' are 'tools available for the resolution of a doubt' about the meaning of a statute." *Almendarez-Torres* v. *United States*, 523 U.S. 224, 234 (1998) (quoting *Brotherhood of R.R. Trainmen* v. *Baltimore & O.R.R.*, 331 U.S. 519, 528-29 (1947)). "[T]he title of a statute or section can aid in resolving an ambiguity in the legislation's text." *INS* v. *National Center for Immigrants' Rights, Inc.*, 502 U.S. 183, 189 (1991). By carving out P2P pirates, the D.C. Circuit has left the statute useless for its intended purpose.

Stripped of the ability to subpoena service providers for the names of individuals using peer-to-peer services to commit copyright infringement, copyright owners are left with two cruder, more costly, and ultimately ineffective options: (1) to

bring suits for contributory and vicarious copyright infringement against the providers of peer-to-peer services; or (2) to file anonymous "John Doe" suits against copyright infringers and obtain their names through subpoenas issued under the procedures of Fed. R. Civ. P. 45.

Despite some initial successes, *see A & M Records, Inc.* v. *Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *In re Aimster Copyright Litig.*, 334 F.3d 643 (7th Cir. 2003), copyright owners' attempts to utilize the former alternative so far have failed to stop the newest and most popular devices for P2P piracy. *See, e.g., Metro-Goldwyn-Mayer Studios, Inc.* v. *Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1046 (C.D. Cal. 2003) (granting summary judgment to two P2P file-copying services, rejecting claims of contributory and vicarious infringement), *appeal pending*, No. 03-55894 (9th Cir., argued Feb. 3, 2004). Nor have any of these efforts stemmed the direct infringement that each of those courts acknowledged is occurring.

"John Doe" suits are no substitute, either. Such suits have faced significant obstacles that threaten to impose substantial and unnecessary costs on both the courts and litigants. As the District Court recognized, requiring copyright owners to file "John Doe" actions simply to learn who the infringer is imposes costs that will "likely undermine the determination of copyright owners to prosecute such actions." Pet. App. 45a. Worse, the costs of such actions have just increased dramatically. Recent decisions in district courts across the country have held that copyright owners may not bring unified actions seeking the identities of numerous "John Doe" customers of a single ISP, but rather must instead sue each individual infringer separately. *See BMG Music et al.* v. *Does 1-203*, No. 04-650 (E.D. Pa. Mar. 5, 2004) (prohibiting joinder and requiring two-hundred and three separate John Doe complaints); *Interscope Records* v. *Does 1-25*, No. 6:04-CV-197-ORL-22-DAB (M.D. Fla. Apr. 27, 2004). As the District Court pointed out, "there is absolutely nothing in the

DMCA or its history to indicate that Congress contemplated copyright owners utilizing John Doe actions in federal court to obtain the identity of apparent infringers." Pet. App. 45a.

Nor are those the only difficulties. Congress in § 512(h) anticipated that identifying the wrongdoers would not only be inexpensive but quick—three times in the provision, as the District Court noted, Congress directed that the subpoena be processed in an "expeditious" manner. Pet. App. 35a. This critical feature allowed copyright owners to confront pirates who, for example, post stolen copies of films before they have been released in threaters. By the time the "John Doe" process has run its course, the prospect for the prompt and effective enforcement Congress anticipated is lost.

If the D.C. Circuit decision stands, in the place of a single subpoena to an Internet service provider like respondent Verizon, a copyright owner now must file hundreds, possibly thousands, of separate complaints and pursue hundreds, possibly thousands, of separate subpoenas. In the place of the expedited procedures of 17 U.S.C. § 512(h), copyright owners (and district courts throughout the country) must now contend with the lengthy process of pursuing third-party discovery. In the meantime, illegal copies of the latest motion pictures, sound recordings and other copyrighted works will surface on the Internet and will rapidly proliferate worldwide, causing inestimable and irreparable losses for the creative industries.

IV. THE URGENCY AND IMPORTANCE OF THIS CRIME WAVE CALL FOR CERTIORARI NOW.

A. Entire Industries Are Threatened.

This Court on several occasions has granted certiorari in order to "consider an important question under the Copyright Act." *E.g.*, *Fortnightly Corp.* (cable retransmission of television programming); *Mills Music, Inc.* v. *Snyder*, 469 U.S. 153, 163 (1985) ("to resolve . . . important question of copyright law"); *De Sylva* v. *Ballentine*, 351 U.S. 570, 572

(1956) ("great importance of these questions in the administration of the Copyright Act").

Seldom does an opinion construing a federal statute have such sweeping effect, both in terms of numbers of people affected, dollars at stake, and the future of a major American industrial sector. All of those are considerations to which this Court has looked in granting review. *E.g.*, *Robert C. Herd & Co.* v. *Krawill Machinery Corp.*, 359 U.S. 297, 300 (1959) ("importance to the shipping industry"); *Commissioner* v. *Lincoln Savings & Loan Ass'n*, 403 U.S. 345, 346-47 (1971) ("importance of the issue for the savings and loan industry"); *SEC* v. *Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 185 (1963) ("importance to the investing public and the financial community"); *National Broiler Marketing Ass'n* v. *United States*, 436 U.S. 816, 820 (1978) ("importance of the issue for the agricultural community and for the administration of the antitrust laws"). *See also United States* v. *Zazove*, 334 U.S. 602, 614 n.17 (1948) ("the added potential liability under the holding of the Circuit Court of Appeals might well amount to billions of dollars"); *United States* v. *Mitchell*, 463 U.S. 206, 211 n.7 (1983) (certiorari granted because "[t]he Government has informed us that the damages claimed in this suit alone may amount to $100 million").

B. The Court of Appeals' Decision Rejects the Interpretation of the Statute by the Copyright Office.

Certiorari is all the more called for when, as here, the interpretation by the Court of Appeals contradicts that of the expert agency assigned to administer the copyright laws, indeed, the agency that was ultimately involved in the negotiation and drafting. "[T]he Copyright Office agrees with the district court's interpretation of Section 512(h)." Pet. App. 133a; *see also id.* at 142a.

> "[A]s the District Court pointed out, subsection 512(h) 'is written without limitation or restriction as to

> its application.' It does not require that a notice be delivered. Had Congress wished to limit the application of the subpoena power, it would simply have said so in the law. It did not.
>
> "The statutory text confirms the policy of compromise behind subsection 512—that copyright owners and ISPs work together to remedy infringement. Limiting the subsection 512(h) subpoena provisions as some have proposed would remove an important tool that parties need to remedy infringement efficiently in the peer-to-peer context."

Pet. App. 143a (statement of Register of Copyrights, September 9, 2003) (footnote omitted). *Cf., e.g., Yellow Transp., Inc.* v. *Michigan*, 537 U.S. 36, 38-39 (2002) (Intermodal Surface Transportation Efficiency Act); *United States* v. *Riverside Bayview Homes, Inc.*, 474 U.S. 121, 126 (1985) (Clean Water Act).

C. The Court of Appeals' Decision Rejects the Interpretation of the Statute by the United States.

In a case involving the very same provision of the DMCA, argued in the Eighth Circuit last week, the United States told that court that the D.C. Circuit's "analysis of the statutory language is incorrect" and "perverse" and "fundamentally alter[s]" the compromise enacted in the DMCA and eliminates "the *quid pro quo* exacted by Congress in return for immunity." Brief for the United States as Intervenor and *Amicus Curiae*, *Recording Industry Ass'n* v. *Charter Communications, Inc.*, No. 03-3802 (8th Cir., argued June 14, 2004), at 17, 18. "[W]hen Congress identified the entities that are subject to subpoenas under Section 512(h), it used unqualified language that encompasses all ISPs and embraces, rather than excludes, ISPs engaged in data transmission." *Id.* at 20. Further:

> "Although Congress may not have foreseen the specific problem of illegal peer-to-peer file transfers, it

> manifestly did anticipate the general problem of which peer-to-peer transfers are simply one instance—the problem of online copyright infringement in which an ISP serves only as a conduit."

Id. at 13-14.

D. There Is No Reason for Delay.

This petition involves a pure legal issue—whether, as the Court of Appeals held, § 512(h) by implication prevents copyright holders from obtaining subpoenas as the DMCA provided they could. That issue is not peculiar to the facts of any particular case. The same issue, as noted, is also before the Eighth Circuit (where a district court rejected the D.C. Circuit's position) and in a district court in the Fourth Circuit. But no matter how those cases are resolved, the issue will not go away so long as the D.C. Circuit's decision stands. It is national in scope and will have to be resolved by this Court. As the District Court observed, the value of copyrighted works "could plummet" under the interpretation adopted by the D.C. Circuit, by which "universal downloading could continue unabated." Pet. App. 106a. With the continuing damage to property and to the honest public, and with Americans' respect for the rule of law further diminishing every day, this Court should address this issue of fundamental importance to the Twenty-First Century now.

CONCLUSION

For the reasons stated herein and in the petition, certiorari should be granted.

Respectfully submitted,

STEVEN J. METALITZ
ERIC J. SCHWARTZ

SMITH & METALITZ LLP
1747 Pennsylvania Avenue, N.W.
Suite 825
Washington, D.C. 20006
(202) 833-4198

Attorneys for Other Amici Curiae

JOHN G. KESTER *
PAUL B. GAFFNEY
JOSEPH M. TERRY

WILLIAMS & CONNOLLY LLP
725 12th Street, N.W.
Washington, D.C. 20005
(202) 434-5069

Attorneys for Amicus Curiae Motion Picture Association of America, Inc.

* Counsel of Record

June 25, 2004

Supreme Court, U.S.
FILED
JUN 2 5 2004
OFFICE OF THE CLERK

No. 03-1579

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,
Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,
Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the District of Columbia Circuit

TIME WARNER'S BRIEF *AMICUS CURIAE* IN SUPPORT OF PETITIONER

HENK BRANDS
Counsel of Record
JOHN H. LONGWELL
PAUL, WEISS, RIFKIND,
WHARTON & GARRISON LLP
1615 L Street, N.W.
Washington, D.C. 20036
(202) 223-7300

Counsel for Amicus Curiae
Time Warner Inc.

June 25, 2004

TABLE OF CONTENTS

	Page
INTEREST OF *AMICUS CURIAE*	1
ARGUMENT	2
I. THE QUESTION PRESENTED IS OF CRUCIAL SIGNIFICANCE TO IMPORTANT SECTORS OF THE U.S. ECONOMY.	3
II. THE COURT OF APPEALS' CONSTRUCTION OF THE STATUTE IS CLEARLY IN ERROR	8
A. The Court of Appeals' Construction Ignores the Legislative Compromise Embodied in the Plain Text of the Statute	8
B. The Court of Appeals' View of the Structure of the Statute Is in Error .	11
C. The Court of Appeals Erred in Relying on a Supposed Contrast Between Subsections (c)(3)(A)(iii) and (j)(1)(A) .	13
CONCLUSION	17

TABLE OF AUTHORITIES

Page

CASES

A & M Records, Inc. v. Napster, Inc.,

114 F. Supp.2d 896 (N.D. Cal. 2000) 10

239 F.3d 1004 (9th Cir. 2001) 3

American Hosp. Ass'n v. NLRB, 499 U.S. 606 (1991) 15

Fort Stewart Schools v. FLRA, 495 U.S. 641 (1990) 15

Griffin v. Oceanic Contractors, Inc., 458 U.S. 564 (1982) 12

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp.2d 1029 (C.D. Cal. 2003), *appeal docketed*, Nos. 03-55894, *et al.* (9th Cir. May 29, 2003) 5

National Cable & Telecomms. Ass'n v. Gulf Power, 534 U.S. 327 (2002) 12

Ratzlaf v. United States, 510 U.S. 135 (1994) 12

Udall v. Tallman, 380 U.S. 1 (1965) 17

United States v. Turkette, 452 U.S. 576 (1981) 12

Whitman v. American Trucking Ass'ns, Inc.,
531 U.S. 457 (2001) 15

STATUTES

17 U.S.C. § 512 . . . . . *passim*

17 U.S.C. § 512(a) 12, 16

17 U.S.C. § 512(b) 11, 12

17 U.S.C. § 512(b)(2)(E) 12

17 U.S.C. § 512(c) 11, 12

17 U.S.C. § 512(c)(1)(C) 9

17 U.S.C. § 512(c)(3)(A) . . . . . *passim*

17 U.S.C. § 512(c)(3)(A)(iii) . . . . . *passim*

17 U.S.C. § 512(d) 11, 13

17 U.S.C. § 512(f) 9

17 U.S.C. § 512(g) 9

17 U.S.C. § 512(h) . . . . . *passim*

17 U.S.C. § 512(h)(1) 6, 11

17 U.S.C. § 512(h)(2)(A) 11, 12

17 U.S.C. § 512(h)(3) 9

17 U.S.C. § 512(h)(4) 6

17 U.S.C. § 512(i) 9

17 U.S.C. § 512(j) 15

17 U.S.C. § 512(j)(1)(A) 13, 14

17 U.S.C. § 512(j)(1)(A)(i) 15, 16

17 U.S.C. § 512(j)(1)(A)(ii) 15, 16

17 U.S.C. § 512(j)(1)(B)(i) 14, 16

17 U.S.C. § 512(j)(2)(D) 16

17 U.S.C. § 512(k)(1)(A) 11

17 U.S.C. § 512(k)(1)(B) 11

17 U.S.C. § 512(m)(2) 16

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) . . 1

LEGISLATIVE MATERIALS

H.R. Rep. No. 105-551(II) (1998) 6

S. Rep. No. 105-190 (1998) 9

OTHER MATERIALS

John Ward Anderson, *Techno-Rebels in West Bank?; File Swapping Firm Claims Odd Hide-Out*, Wash. Post, Feb. 22, 2004, at A29, *available at* 2004 WL 55840419 3

Bruce B. Auster, *I Want My MP3, But Who Pays the Bill? Closing Napster Won't Kill Digital Music Online*, U.S. News & World Rep., Feb. 26, 2001, at 44, *available at* 2001 WL 6319789 5

Mike France, *Music Pirates, You're Sunk*, Bus. Wk., Sep. 8, 2003, at 40, *available at* 2003 WL 62195471 6

Mike France, *Striking Back; How the Music Industry Charted its Crusade Against Web Pirates*, Bus. Wk., Sep. 29, 2003, at 94, *available at* 2003 WL 62195792 5

Ronald Grover & Heather Green, *The Digital Age Presents Hollywood Heist, Will Tinseltown Let Techies Steal the Show?*, Bus. Wk., July 14, 2003, at 74, *available at* 2003 WL 8815656 . . 3

Doug Mellgren, *Teen A Villain To Hollywood*, L.A. Times, Mar. 11, 2001, at B1, *available at* 2001 WL 2468652 4

Amanda Ripley, *Hollywood Robbery; How Does a Hit Movie Go From the Free Market to the Black Market?*, Time Mag., Jan. 26, 2004, at 56, *available at* 2004 WL 61549448 4

Ethan Smith, *Music Industry's Move Against Swappers Hits a Snag Just as Impact Takes Hold*, Wall St. J., Dec. 22, 2003, at B1, *available at* 2003 WL-WSJ 68131582 . . . . . 5, 6

Kenneth Terrel & Seth Rosen, *A Nation of Pirates*, U.S. News & World Rep., July 14, 2003, at 40, *available at* 2003 WL 2022009 3

Tipping Hollywood the Black Spot — The Digital Threat to Hollywood, Economist, Aug. 30, 2003, at 43, *available at* 2003 WL 58583842 4

Brief for the United States as Intervenor and *Amicus Curiae*, *RIAA v. Charter Communications, Inc.*, No. 03-3802, at 31-32 (8th Cir. filed Feb. 24, 2004), *available at* http://www.ca8.uscourts.gov/briefs/04/03/intervenor/033802_1br. pdf?A1=View+Brief. 10, 17

TIME WARNER'S BRIEF *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

Time Warner Inc. ("Time Warner") respectfully submits this brief *amicus curiae* in support of petitioner.[1]

INTEREST OF *AMICUS CURIAE*

This case involves a dispute between copyright holders, on one side, and Internet service providers ("ISPs"), on the other. The petitioner, RIAA, representing copyright holders, seeks access to the identities of persons who engage or have engaged in the on-line exchange of music recordings through so-called file-swapping on "peer-to-peer" systems like KaZaA, Morpheus, and Grokster. RIAA invoked the subpoena process of the Digital Millennium Copyright Act ("DMCA"), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in various provisions of Title 17). The respondent, Verizon, a major ISP, agrees that file-swapping violates copyright law. It also agrees that it can be made to divulge its subscribers' identities in so-called "John Doe" actions. But it resists the DMCA's more expeditious subpoena procedure.

Time Warner is uniquely situated to appreciate the parties' positions: it has interests on both sides of this dispute. Time Warner is one of the world's largest copyright holders, being the parent company of Warner Bros. Pictures, Warner Home Video, Warner Bros. Television Production, New Line Cinema, Turner Broadcasting System, various local news channels, Home Box Office, The WB Network, Time Inc., and Time Warner Book Group

---

[1] No counsel for a party authored this brief in whole or in part, and no person or entity other than *amicus curiae* has made a monetary contribution to the preparation or submission of this brief. Petitioner and respondent have consented to the filing of this brief. We have filed their consent letters with the Clerk of the Court.

(owner of Warner Books and Little, Brown and Company).[2] At the same time, Time Warner is also the parent company of the Nation's largest provider of Internet access service, America Online, which has some 24 million dial-up and broadband subscribers. In addition, another Time Warner subsidiary, Road Runner, provides high-speed Internet service to more than 3 million subscribers of Time Warner Cable.

As the parent company both of copyright-holding entities and of ISPs, Time Warner brings a unique perspective to this dispute that it believes may be valuable to the Court. Some ISPs may undervalue the harm illegal file-swapping inflicts on copyright owners and may have little incentive to refrain from advocating positions that would unduly hamper copyright owners' efforts to enforce their rights. Conversely, copyright owners may assign little weight to burdens imposed on ISPs and may have little incentive to refrain from advocating positions that would impose unwarranted costs. By contrast, Time Warner's interest lies in a balanced result that will protect the interests of copyright holders in the battle against online piracy, while ensuring that ISPs do not face unreasonable burdens and costs.

ARGUMENT

The purpose of this brief is not to repeat the legal arguments made in the RIAA's well-reasoned petition for a writ of certiorari, with which Time Warner agrees. Rather, the purpose of this brief is to underscore and illustrate the practical significance of the legal issues at stake from the perspective of a firm with interests on both

---

[2] In a transaction that closed in March 2004, Time Warner sold its interest in Warner Music Group Inc. and its affiliated music companies.

the copyright-owner and ISP sides of the case. In addition, we will further highlight the erroneous nature of particular aspects of the court of appeals' legal analysis.

I. THE QUESTION PRESENTED IS OF CRUCIAL SIGNIFICANCE TO IMPORTANT SECTORS OF THE U.S. ECONOMY.

There is no question that the unauthorized copying of copyrighted works via "peer-to-peer" systems like KaZaA, Morpheus, and Grokster constitutes illegal copyright infringement on a massive and unprecedented scale. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013-14 (9th Cir. 2001). "Every day, ordinary people download billions of files: blockbuster movies, cable TV shows, music, video games, software, and nearly every other kind of copyright-protected material available in digital form." Kenneth Terrel & Seth Rosen, *A Nation of Pirates*, U.S. News & World Rep., July 14, 2003, at 40, *available at* 2003 WL 2022009.

This illegal file-swapping has taken a severe toll on the music industry: "Only five years ago, music sales were booming. Today, the industry is nearly paralyzed by piracy." Ronald Grover & Heather Green, *The Digital Age Presents Hollywood Heist, Will Tinseltown Let Techies Steal the Show?*, Bus. Wk., July 14, 2003, at 74, *available at* 2003 WL 8815656. "According to the RIAA, about 2.6 billion copyrighted files, mostly songs, are downloaded over the Internet per month, which the organization says is the leading cause of the worldwide decline in music industry sales from $40 billion in 2000 to $26 billion in 2002." John Ward Anderson, *Techno-Rebels in West Bank?; File Swapping Firm Claims Odd Hide-Out*, Wash. Post, Feb. 22, 2004, at A29, *available at* 2004 WL 55840419; *see generally* Pet. 18 ("retail sales

of music have plummeted, falling 7% in 2000, 10% in 2001, 11% in 2002, and 7% in 2003").

The threat is just as great for the movie industry: "Already as many as 600,000 movie files are shared each day on peer-to-peer file-sharing networks such as Morpheus and Grokster, according to the Motion Picture Association of America (MPAA). That number is likely to soar as more households get broadband internet and compression technology cuts download time." *Tipping Hollywood the Black Spot — The Digital Threat to Hollywood*, Economist, Aug. 30, 2003, at 43, *available at* 2003 WL 58583842; *see also* Pet. App. 137a ("With broadband connections becoming more and more widespread, it is increasingly more common that the larger files containing full-length motion pictures are copied back and forth.") (footnote omitted). "Last year the film industry . . . would have made $3.5 billion more if not for piracy . . . . Next year the loss may rise to $5.4 billion." Amanda Ripley, *Hollywood Robbery; How Does a Hit Movie Go From the Free Market to the Black Market?*, Time Mag., Jan. 26, 2004, at 56, *available at* 2004 WL 61549448. Piracy "hands the keys to the castle to copyright pirates, hurting the livelihood of thousands of people, from big-name stars to grips, gaffers and carpenters." Doug Mellgren, *Teen A Villain To Hollywood*, L.A. Times, Mar. 11, 2001, at B1, *available at* 2001 WL 2468652 (internal quotation marks omitted).

The most natural targets of copyright owners' efforts to enforce their rights are the purveyors of peer-to-peer software and operators of file-swapping networks, who seek to profit from this illegal activity primarily by selling advertising. But pursuing such entities does not hold out a complete solution: to the extent that they can be shut down or controlled at all (some have relocated to exotic

locations, *see* Pet. 18 n.15), new ones inevitably appear.[3] Moreover, closing down these entities does not necessarily eliminate the problems that they create: "Unlike Napster, which relied upon a centralized communication architecture to identify the .mp3 files available for download, the current generation of P2P file sharing programs allow an internet user to search directly the .mp3 file libraries of other users; no web site is involved." Pet. App. 3a; *see also Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp.2d 1029, 1041-43 (C.D. Cal. 2003) (holding — mistakenly in our view — that certain peer-to-peer systems' structure avoids secondary infringement), *appeal docketed*, Nos. 03-55894, *et al.* (9th Cir. May 29, 2003).

That is why the music industry was forced to pursue file-swappers with lawsuits. *See generally* Pet. App. 140a. In the wake of these lawsuits, the use of peer-to-peer services began to wane, and music sales rebounded. *See* Pet. 27 n.18; *see also* Ethan Smith, *Music Industry's Move Against Swappers Hits a Snag Just as Impact Takes Hold*, Wall St. J., Dec. 22, 2003, at B1, *available at* 2003 WL-WSJ 68131582 ("the three-year slide in music sales began to slow dramatically on almost precisely the same date the suits [against swappers] were filed, amid massive publicity"); Mike France, *Music Pirates, You're*

---

[3] *See* Mike France, *Striking Back; How the Music Industry Charted its Crusade Against Web Pirates*, Bus. Wk., Sep. 29, 2003, at 94, *available at* 2003 WL 62195792 ("Though lawyers shut down Napster in July, 2001, other peer-to-peer networks carefully designed to skirt the law, such as Morpheus and Grokster, quickly rose up in its wake."); Bruce B. Auster, *I Want My MP3, But Who Pays the Bill? Closing Napster Won't Kill Digital Music Online*, U.S. News & World Rep., Feb. 26, 2001, at 44, *available at* 2001 WL 6319789 ("No matter how good the technology, the industry won't be able to chase and close every last free-music site.").

Sunk, Bus. Wk., Sep. 8, 2003, at 40, *available at* 2003 WL 62195471 ("After the number of households downloading music from the Internet climbed to a high of 14.5 million in April, it dwindled to 12.7 million in May and 10.4 million in June, according to market researcher NPD Group Inc.").

The music industry was able to mount such an effective campaign in important part because of the DMCA's subpoena provision, 17 U.S.C. § 512(h). As the court of appeals noted, copyright owners "can readily obtain the screen name of an individual user, and using the Internet Protocol (IP) address associated with that screen name, can trace the user to his ISP. Only the ISP, however, can link the IP address used to access a P2P program with the name and address of a person — the ISP's customer — who can then be contacted or, if need be, sued by the RIAA." Pet. App. 3a; *see also* Pet. 10; Pet. App. 18a. Section 512(h) bridges that gap by allowing copyright owners to "request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer." 17 U.S.C. § 512(h)(1).

This procedure is plainly more efficient than the alternative, filing so-called "John Doe" lawsuits against an anonymous infringer and requesting expedited third-party discovery against the infringer's ISP. That option does not yield the infringer's name as quickly as a Section 512(h) subpoena, which is precisely why Congress created Section 512(h)'s more "expeditiou[s]" procedure. *Id.* § 512(h)(4); *see also* H.R. Rep. No. 105-551(II), at 61 (1998) ("The issuing of the order should be a ministerial function performed quickly for this provision to have its intended effect."). Given the "ease with which digital works can be copied and distributed worldwide virtually instantaneously," Pet. App. 35a-36a, any delay can harmfully "undermine the ability of copyright owners to act

quickly to prevent further infringement of their copyrights." *Id.* at 45a. Indeed, the delay attendant upon John Doe suits can altogether defeat recourse when ISPs fail to retain identifying information. *See* Pet. 27, 28.

Quite apart from the delay inherent in John Doe suits, they are less efficient. For one thing, John Doe suits impede settlement. Whereas the DMCA's subpoena mechanism allows parties to seek a resolution short of filing suit, that is not an option with John Doe suits: the only way to identify the infringer is by filing an actual lawsuit. For another thing, John Doe suits bring additional "effort and expense" for copyright holders, Pet. App. 45a, and place a heavy "burden on the federal courts," *id.* at 45a-46a.

Time Warner recognizes that DMCA subpoenas may impose a compliance burden on ISPs, *see id.* at 34a — a burden of which it has borne the full brunt in its America Online and Road Runner businesses. Particularly when large numbers of subpoenas are being served within short periods of time, compliance with Section 512(h) requires a dedication of substantial resources. For example, for every subpoena, ISP employees need to conduct a complex process to identify the subscriber involved. In addition, the ISP's law department typically reviews subpoenas and, as a matter of practice, sends prompt notification to customers. Because of this burden, Time Warner believes that ISPs must be granted a reasonable time to respond and, in appropriate cases, should be compensated for their assistance in accordance with applicable procedural rules.

That said, Time Warner believes that the DMCA process as it functioned prior to the decision below properly balanced the interests of ISPs and copyright holders by limiting ISPs' liability for subscribers' acts of copyright

infringement while requiring ISPs to assist in combating online infringement, including by identifying infringing subscribers through the streamlined DMCA subpoena process. The DMCA accomplishes this while providing "substantial protection to service providers and their customers against overly aggressive copyright owners and unwarranted subpoenas." Pet. App. 47a.

The D.C. Circuit's decision threatens to derail efforts of copyright holders to protect their legal rights and staunch the flow of Internet piracy. Without a quick and efficacious way of identifying file-swappers, it is difficult to curb piracy in an effective way. And, unless Internet piracy is brought under control, the copyright-intensive music and movie industries will continue to suffer serious harm. Indeed, ISPs themselves, to the extent they attract customers by making available copyrighted materials lawfully, are harmed by the massive piracy currently in progress. In each of the industries affected, substantial amounts of risk-bearing investment and numerous well-paying jobs hang in the balance. The petition thus raises issues of vital importance to large sectors of the Nation's economy. It should be granted for that reason alone.

II. THE COURT OF APPEALS' CONSTRUCTION OF THE STATUTE IS CLEARLY IN ERROR.

Review is particularly warranted because the D.C. Circuit's construction of Section 512(h) is plainly incorrect.

A. The Court of Appeals' Construction Ignores the Legislative Compromise Embodied in the Plain Text of the Statute.

Title II of the DMCA enacted a carefully calibrated compromise between interests of copyright holders and

interests of ISPs.[4] "Congress attempted to balance the liability protections for service providers with the need for broad protection of copyrights on the Internet." Pet. App. 38a. Thus, for example, Congress conditioned ISPs' immunity from damages upon their taking down certain infringing material, *see, e.g.*, 17 U.S.C. § 512(c)(1)(C), and terminating the accounts of certain repeat infringers, *see id.* § 512(i).[5] And, of particular interest for purposes of this case, Congress required ISPs "to expeditiously disclose" the identity of infringing subscribers in response to a special subpoena. *See id.* § 512(h)(3).

Speaking as a company that is both a major ISP and a major copyright holder, we find it utterly implausible that Congress would have wanted to reconcile the interests of the stakeholder groups by exempting "conduit" ISPs (*i.e.*, ISPs transmitting infringing material at the behest of subscribers) from the subpoena provision. As the district court correctly put it: "There is no discernable reason why Congress would limit the subpoena authority under subsection (h) to subsection (c) service providers alone." Pet. App. 34a; *see id.* at 41a-42a ("There is no logical connection between the line Verizon seeks to draw and the objectives Congress sought to achieve through the DMCA."). Indeed, the court of appeals identified no such reason.

---

[4] *See, e.g.*, S. Rep. No. 105-190, at 9 (1998) ("Title II . . . reflects 3 months of negotiations supervised by Chairman Hatch and assisted by Senator Ashcroft among the major copyright owners and the major . . . ISP's.").

[5] Congress balanced these requirements with liability for infringement notices containing knowing and material misrepresentations, *see* 17 U.S.C. § 512(f), and a "put back" procedure for material erroneously identified as infringing, *see id.* § 512(g).

That failure is particularly troubling because, even at the time the DMCA was enacted in 1998 (one year before Napster, the first peer-to-peer system, burst onto the scene in 1999[6]), Internet users *were* making copyrighted materials available for illegal copying from their own computers.[7] It would have been strange, to say the least, for a Congress so well-informed by the major industry participants to allow use of the subpoena process to combat piracy on ISP servers but somehow to exempt piracy on home computers. That approach would deny copyright owners access to the subpoena process precisely when they need it most: whereas copyright owners can stop server-based copyright infringement simply by pursuing an easily-identifiable ISP, they can stop home-computer-based infringement only if an ISP helps them identify its anonymous subscriber.

Moreover, if Congress had meant to immunize conduit ISPs from the DMCA's subpoena reach, one would have expected to see some sign of it in Section 512(h), the provision in which the statute — wholly separate from the four substantive liability limitations — specifically addresses the subpoena topic. Yet Section 512(h) displays no such sign. To the contrary, Section 512(h) broadly proclaims that any "copyright owner" may obtain "a subpoena to a service provider for identification of an alleged infringer." 17 U.S.C. § 512(h)(1). And, for purposes of Section 512(h), the statute defines "service provider"

---

[6] *See A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp.2d 896, 900 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001); *see also* Pet. App. 135a.

[7] *See* Pet. 3-7, 25-26; *see also* Br. for the United States as Intervenor and *Amicus Curiae*, *RIAA v. Charter Communications, Inc.*, No. 03-3802, at 31-32 (8th Cir. filed Feb. 24, 2004), *available at* http://www.ca8.uscourts.gov/briefs/04/03/intervenor/033802_1br.pdf?A1=View+Brief.

broadly enough to include conduit ISPs, *see id.* § 512(k)(1)(B), even though the statute specifically excludes conduit ISPs from the definition for purposes of another subsection, *see id.* § 512(k)(1)(A). That should have been the end of the matter: there is no cause to squint at sections other than Section 512(h) in search of implicit limitations.

B. The Court of Appeals' View of the Structure of the Statute Is in Error.

As the court of appeals pointed out, Section 512(h)(2)(A) requires a subpoena applicant to file "a copy of a notification described in subsection (c)(3)(A)." *Id.* § 512(h)(2)(A). Subsection (c)(3)(A) describes a notification that, among other things, identifies "the material . . . that is to be removed or access to which is to be disabled." *Id.* § 512(c)(3)(A). Clearly, Congress concluded that an ISP receiving a Section 512(h) subpoena should be informed of the nature of the infringement with which its subscriber is charged. That makes good sense: it helps the ISP unearth the requested information and allows it to decide, say, whether it should inform its subscriber of the allegations or whether it should voluntarily block access or terminate the subscriber's account.

But the court of appeals saw in Section 512(h)(2)(A)'s reference to Subsection (c)(3)(A) a structural problem. As the court noted, the notifications described in Subsection (c)(3)(A) serve an immunity-related purpose under Subsections (b), (c), and (d). Under those provisions, the court of appeals said, (c)(3)(A) notifications serve a "notice and take-down" purpose: when a copyright holder sends a (c)(3)(A) notification to an ISP, the ISP must "take down" infringing material if it wishes to claim immunity under Subsections (b), (c), and (d). *See* Pet. App.

8a, 13a.[8] By contrast, Subsection (a) does not condition immunity on remedial steps in response to a "take down" notice. *See* Pet. App. 8a. The court of appeals concluded that, because a conduit ISP thus cannot be sent a (c)(3)(A) notification that is "effective" to trigger immunity-related duties, Congress could not have intended subpoenas to be available against conduit ISPs. *Id.* at 14a.

But just as courts must not disregard plain statutory language on the basis of their reading of legislative history, *see Ratzlaf v. United States*, 510 U.S. 135, 147-48 (1994), so courts must not disregard plain statutory language on the basis of vague structural notions unless "the literal application of a statute will produce a result demonstrably at odds with the intentions of its drafters." *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982).[9] Perhaps the statutory scheme envisioned by the court of appeals appealed to its desire for systemic tidiness, but that scheme is squarely at odds with the legislative compromise as embodied in the statutory text.

Contrary to the court of appeals' implication, *see* Pet. App. 12a, Section 512(h)(2)(A) does not require a subpoena applicant to file a notification that is "effective under" subsection (c)(3)(A) — it merely requires a notifica-

---

[8] Insofar as subsection (b) is concerned, the court of appeals' premise is only partially correct. That provision requires ISPs to "take down" infringing material only in certain narrowly defined circumstances. *See* 17 U.S.C. § 512(b)(2)(E).

[9] *See also National Cable & Telecomms. Ass'n v. Gulf Power*, 534 U.S. 327, 335 (2002) (rejecting limiting inference based on "the structure of the Act" as being contrary to "the plain language of" the statute's operative sections); *United States v. Turkette*, 452 U.S. 576, 586-87 (1981) (rejecting argument that, because remedies against RICO "enterprises" include divestiture and dissolution, the statute's "structure . . . limits its application to legitimate enterprises").

tion of the kind "described in" that subsection. What emerges from the statutory text is a belief that, as part of the subpoena process, both the clerk of the district court and the ISP involved should receive a description of the offending conduct in a format that was simple, standardized, and containing indicia of reliability. Having already created such a format in subsection (c)(3)(A), Congress likely concluded that, although (c)(3)(A) notifications perform an immunity-related function in subsections (b) through (d), they could just as well serve an informational function in subsection (h). That Congress used the words "described in" indicates that Congress simply sought to incorporate the (c)(3)(A) vehicle by reference.

C. The Court of Appeals Erred in Relying on a Supposed Contrast Between Subsections (c)(3)(A)(iii) and (j)(1)(A).

The court of appeals saw further support for its reading in Subsections (c)(3)(A)(iii) and (j)(1)(A). As already seen, a subpoena applicant must file with the clerk "a copy of a notification described in subsection (c)(3)(A)." 17 U.S.C. § 512(h)(2)(A). And Subsection (c)(3)(A)(iii) requires the copyright holder to identify "material . . . that is to be removed or access to which is to be disabled." *Id.* § 512(c)(3)(A)(iii). According to the court of appeals, a conduit ISP "can neither 'remove' nor 'disable access to' the infringing material because that material is not stored on the ISP's servers." Pet. App. 9a. The court of appeals apparently concluded that this language fits the conduit ISP situation so poorly that Congress could not have intended conduit ISPs to be subject to subsection (h)'s subpoena procedure.

Even if one reads subsection (c)(3)(A)(iii) as indicating that the removing or disabling must be done by the ISP,[10] the provision makes ample good sense. Congress likely thought that, after learning the identity of the subscriber, the copyright holder would seek an injunction against the ISP "restraining the service provider from providing access to [the subscriber] . . . by terminating the accounts of the subscriber." 17 U.S.C. § 512(j)(1)(B)(i). Such an injunction plainly would have the effect of "disabl[ing]" "access" for purposes of subsection (c)(3)(A)(iii): the ordinary meaning of those words is easily broad enough to cover account termination. *See* Pet. App. 33a n.5. Indeed, the court of appeals did not hold otherwise.

Instead, the court of appeals implied that the DMCA gives the words "disabl[ing]" "access" a meaning different from common parlance. It based that conclusion on an unrelated provision, Section 512(j)(1)(A), which provides that an ISP may be subjected to injunctions that prohibit it from either (i) "providing access to infringing material or activity residing at a particular online site on the [ISP's] system or network," or (ii) "providing access to a subscriber . . . who is engaged in infringing activity . . . , by terminating the accounts of the subscriber." 17 U.S.C. § 512(j)(1)(A). According to the court, that distinction signaled that "Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies." Pet. App. 10a.

---

[10] The statutory language is cast in the passive voice. Thus, it is broad enough to refer to material that *the copyright holder* would like to see removed or made inaccessible — say, by, after learning the subscriber's identity, persuading him or her to remove the infringing files, or, failing that, having a court order the subscriber to do so.

Even if Section 512(j) in fact broadcast the signal that the court of appeals thought it received, that signal would be far too faint to overcome the power of Section 512(h)'s clear language. "Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions — it does not, one might say, hide elephants in mouseholes."[11] If Congress had intended to exempt conduit ISPs from Section 512(h)'s coverage, it would have done so directly (say, by excluding them from the definition of "service provider," *see* Pet. App. 31a-32a) — not through a convoluted connect-the-dots approach.

Besides, the signal that the court of appeals thought it received from subsection (j) simply is not there. If Sections 512(c)(3)(A)(iii) and 512(j)(1)(A)(i) had each spoken of "access disabling" whereas Section 512(j)(1)(A)(ii) spoke of "account termination," the court might have had the beginning of a point.[12] But Sections 512(j)(1)(A)(i) and 512(c)(3)(A)(iii) do not use identical terms. Section 512(c)(3)(A)(iii) broadly speaks of "material . . . access to which is to be disabled." 17 U.S.C. § 512(c)(3)(A)(iii). In contrast, Section 512(j)(1)(A)(i)

---

[11] *Whitman v. American Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001); *see also American Hosp. Ass'n v. NLRB*, 499 U.S. 606, 613 (1991) ("As a matter of statutory drafting, if Congress had intended to curtail in a particular area the broad rulemaking authority [it has] granted . . . , we would have expected it to do so in language expressly describing [such] an exception.").

[12] Even that point would not necessarily be persuasive: Congress might have devoted Section 512(j)(1)(A)(ii) to account termination merely out of an abundance of caution — "a drafting imprecision venerable enough to have left its mark on legal Latin (*ex abundanti cautela*)," *Fort Stewart Schools v. FLRA*, 495 U.S. 641, 646 (1990) — simply to dispel any question whether account termination might be available under Section 512(j)(1)(A)(i).

narrowly addresses disabling "access" to one particular kind of "material" — namely, material "residing at a particular online site on the provider's system or network." *Id.* § 512(j)(1)(A)(i). Thus, the two kinds of access disabling described in (j)(1)(A)(i) and (ii) are simply different species of the same "disabl[ing]" "access" genus mentioned in Section 512(c)(3)(A)(iii).[13]

Other subsections confirm this reading. Section 512(j)(1)(A)(ii) indicates that "terminating the accounts of the subscriber" is merely a form of not "providing access." *Id.* § 512(j)(1)(A)(ii); *see also id.* § 512(j)(1)(B)(i). In addition, Section 512(j)(2)(D) requires courts contemplating the issuance of an injunction to consider "whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available," *id.* § 512(j)(2)(D) — thereby indicating that all forms of injunctive relief listed in Subsection (j), including account termination, constitute "means of preventing or restraining access to the infringing material." Finally, Section 512(m)(2) states that the limitation on liability found in subsection (a) does not hinge on the ISP's "removing, or disabling access to material in cases in which such conduct is prohibited by law," *id.* § 512(m)(2) — again indicating that Congress expected conduit ISPs to disable access (presumably by terminating accounts).

* * *

In short, there is no force to either of the two concerns that, according to the court of appeals, stood in the way

---

[13] Similarly, if Section 512(c)(3)(A)(iii) spoke of "men," Section 512(j)(1)(A)(i) spoke of "men who are mortal," and Section 512(j)(1)(A)(ii) spoke of "Greeks," there might be a faint implication (easily overcome by common sense) that Greeks are immortal. But there would be no implication at all that Greeks are not human.

of enforcing Section 512(h)'s plain language. That is why the court of appeals' reasoning has been expressly disavowed by the Copyright Office,[14] whose interpretation is entitled to respect.[15] The court of appeals' error is causing massive injury. Given the size of the harm that is occurring every day to industries that are dependent on copyrights, the luxury of allowing further "percolation" is not affordable. Further review is needed now.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

HENK BRANDS
Counsel of Record
JOHN H. LONGWELL
PAUL, WEISS, RIFKIND,
WHARTON & GARRISON LLP
1615 L Street, N.W.
Washington, D.C. 20036
(202) 223-7300

Counsel for Amicus Curiae
Time Warner Inc.

June 25, 2004

---

[14] *See* Pet. App. 133a-34a, 142a; *see also* Br. for the United States as Intervenor and *Amicus Curiae*, *RIAA v. Charter Communications, Inc.*, No. 03-3802, at 19-27 (8th Cir. filed Feb. 24, 2004), *available at* http://www.ca8.uscourts.gov/briefs/04/03/intervenor/033802_1br.pdf?A1=View+Brief.

[15] *See* Pet. 16 n.14; *see also Udall v. Tallman*, 380 U.S. 1, 16 (1965) (courts must give exceptional deference to "a contemporaneous construction of a statute by the men charged with the responsibility of setting its machinery in motion, of making the parts work efficiently and smoothly while they are yet untried and new") (internal quotation marks omitted).